中科网威 Anysec technology

客户第一 用心服务

ANYSEC-日志审计系统使用说明书

总机电话-- 0755-83658009　技术支持-- 0755-83658229　24 小时技术值班热线-----135-1069-3536
http://www.anysec.com　深圳市龙华区观澜街道观光路 1301-80 号电子科技大学(深圳)高等研究院 3 号楼 1401

声明

本公司对本手册的内容在不通知用户的情况下有更改的权利。

NOTICES

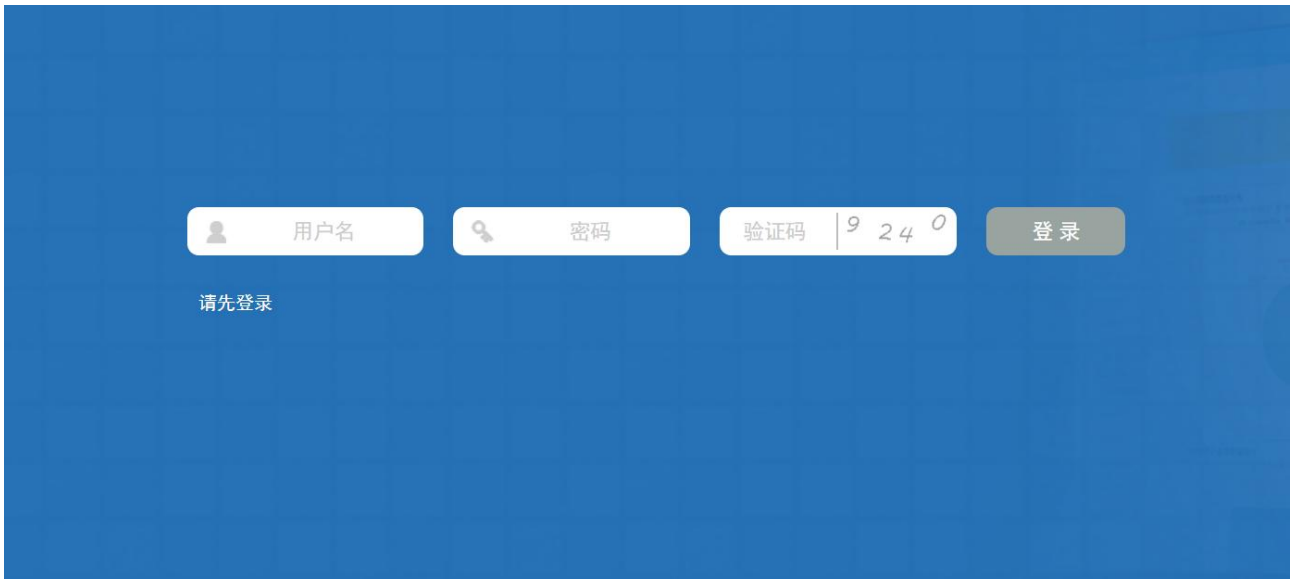
Shenzhen Anysec-Tech Company Limited reserves the right to make any changes in specifications and other information contained in this publication without prior notice and without obligation to notify any person or entity of such revisions or changes.

目录

一. 初始化配置

1.1 Web 管理

在浏览器地址栏输入 ip（https://192.168.1.40）（注：为出厂默认 ip）即可进行访问。默认管理接口是 eth0。根据用户网络环境，在部署时可对访问地址进行灵活修改。



1.2 用户初始账户和密码

系统预设账户列表如下，可根据需要选择登录：

用户类型	用户名	密码
超级管理员	admin	admin123456
操作管理员	operator	operator123456
审计管理员	saudit	saudit123456
账号管理员	userManager	user123456

1.3 权限划分

用户类型	用户所拥有权限
超级管理员	拥有所有权限
操作管理员	除内部审计、用户管理、授权规则的所有功能
审计管理员	只有内部审计权限
账号管理员	只有用户管理权限

二. 首页

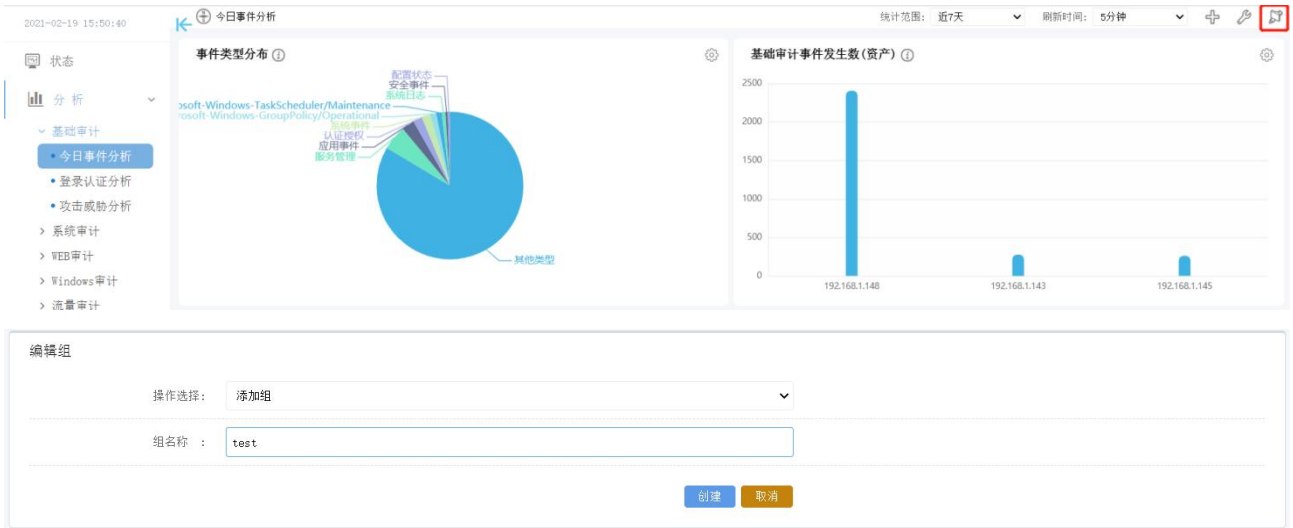
登入系统默认进入首页即‘状态’菜单项，概括显示系统主要统计信息。

三. 分析

点击系统右上角‘编辑组’→选择添加组并填写‘组名称’→点击‘创建’，完成添加分析组操作。如图：

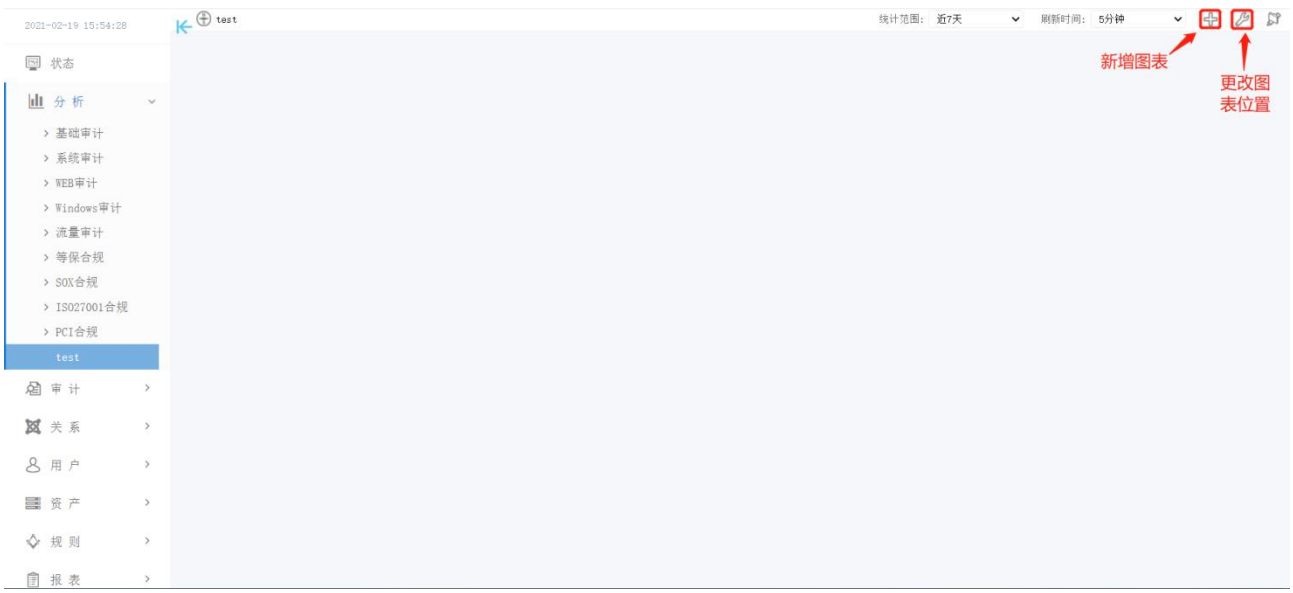
3.1 添加分析组

点击系统右上角‘编辑组’→选择添加组并填写‘组名称’→点击‘创建’，完成添加分析组操作。如图：



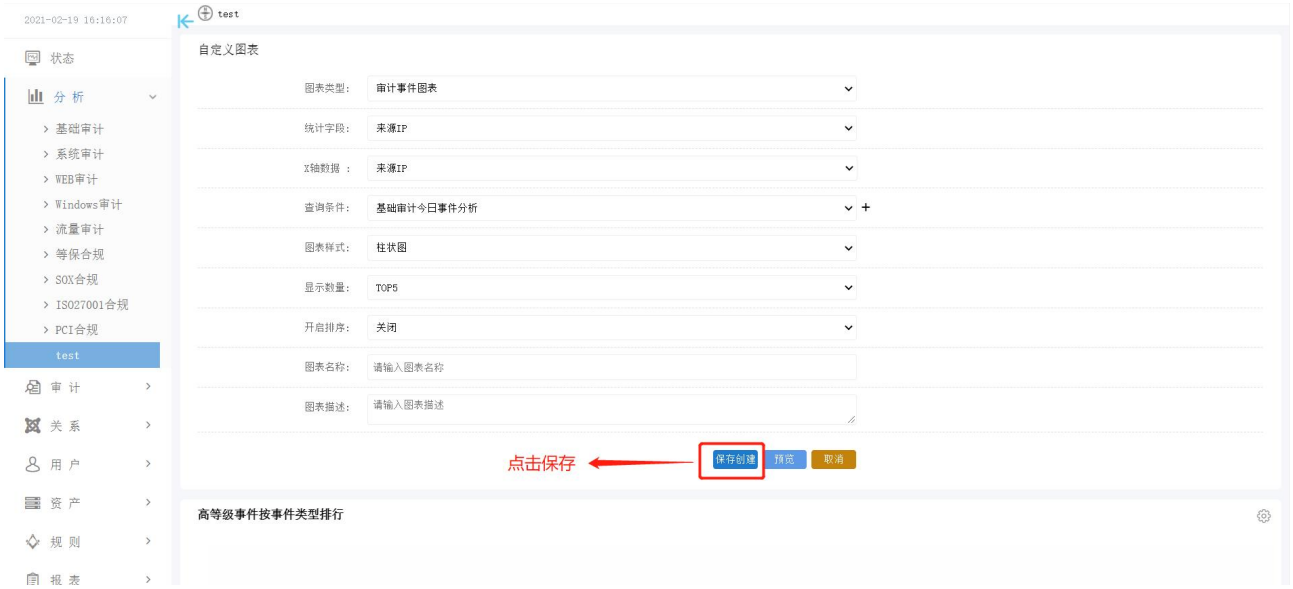
3.2 添加已存在的图表

进入菜单项‘分析’的任意子项，点击右上角‘添加图表’按钮，选择需要添加的图表类型，点击‘保存’完成添加。



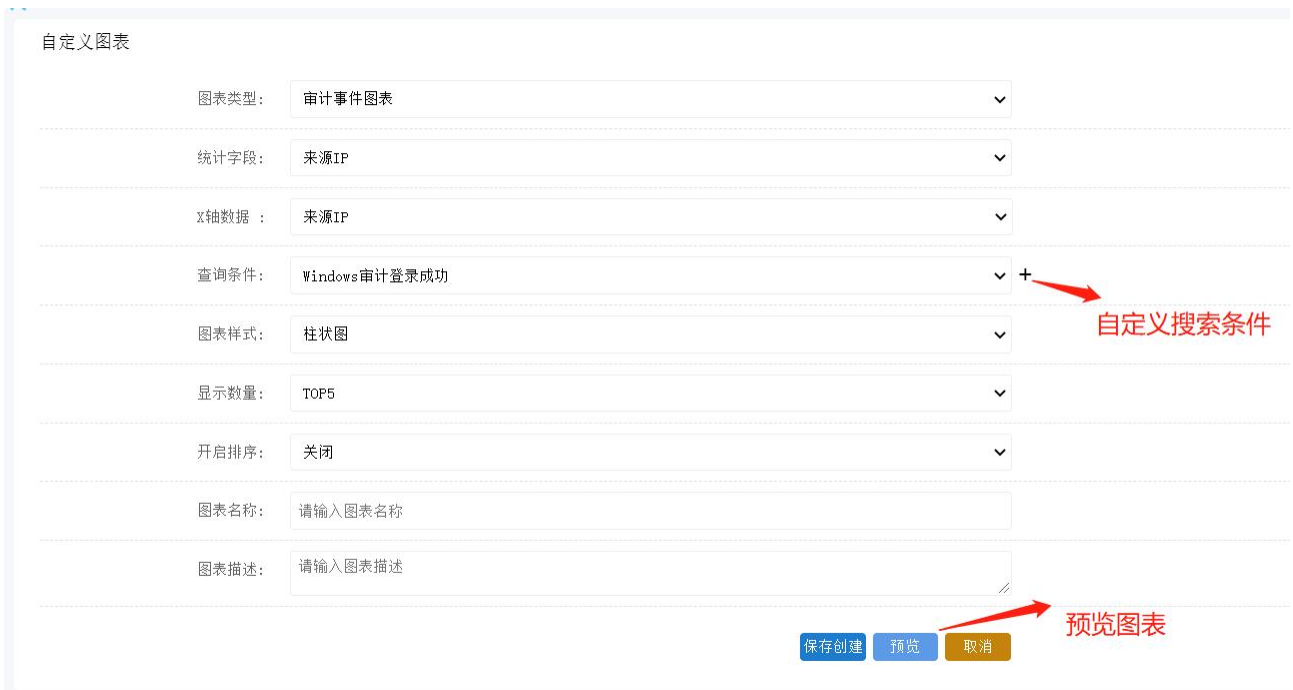
3.3 添加自定义图表

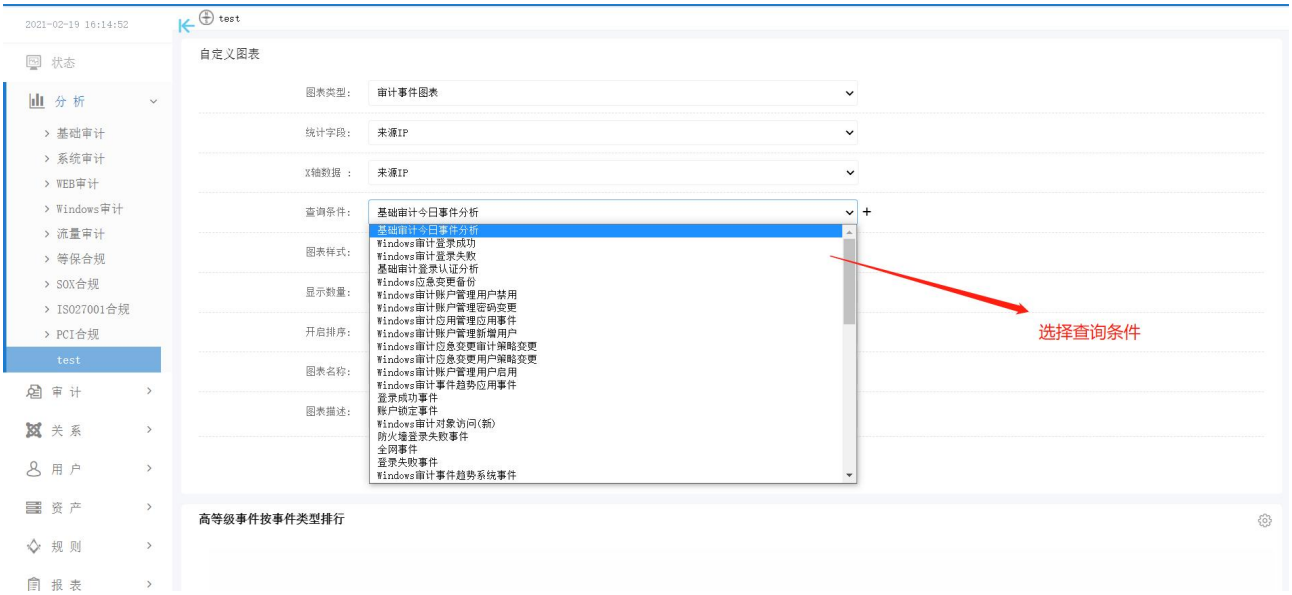
进入菜单项‘分析’的任意子项，点击右上角‘添加图表’按钮，点击‘自定义’进入自定义图表界面，可选择诸如选择统计类型/X 轴/Y 轴/查询条件/图表样式/TOPN/时间范围等数据统计信息，填写图表名，点击‘保存创建’完成自定义图表的操作。



3.4 自定义图表预览功能

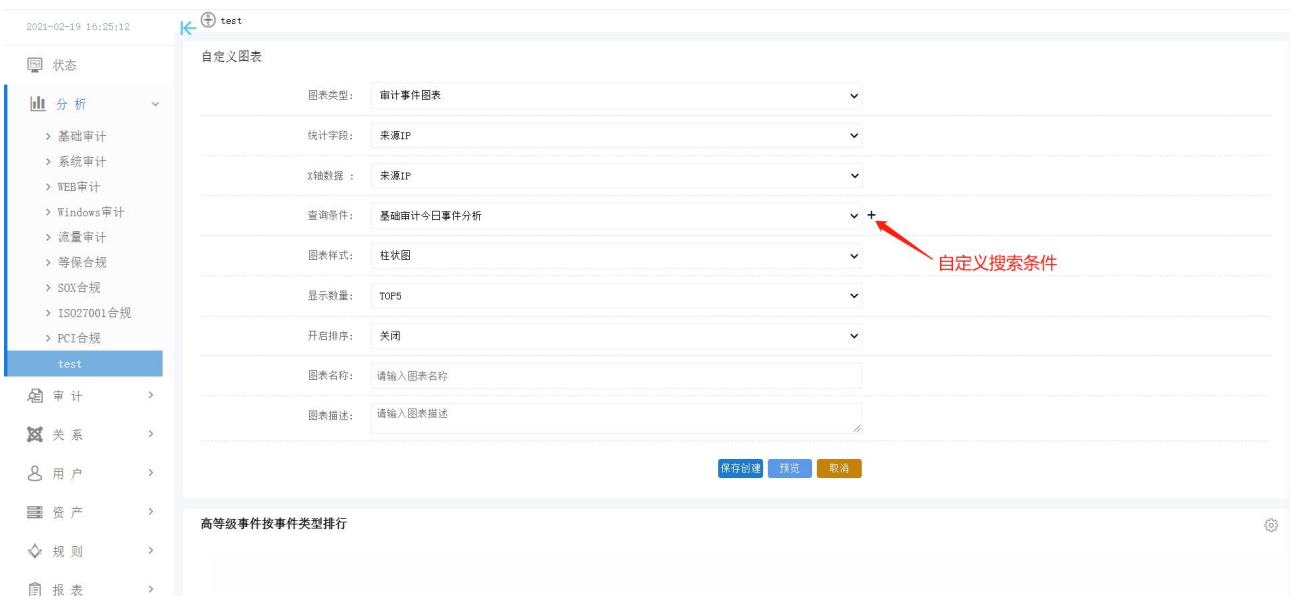
完成添加自定义图表后，可点击‘预览’查看自定义图表，点击‘查看事件’，可自定义搜索条件，如下图：

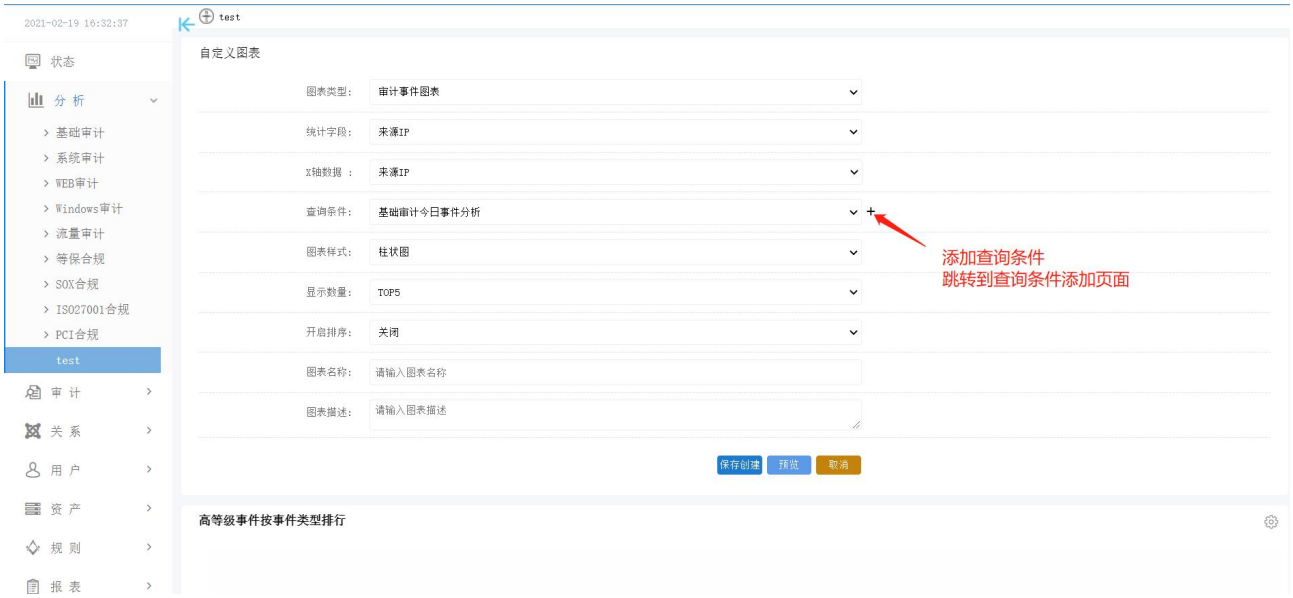


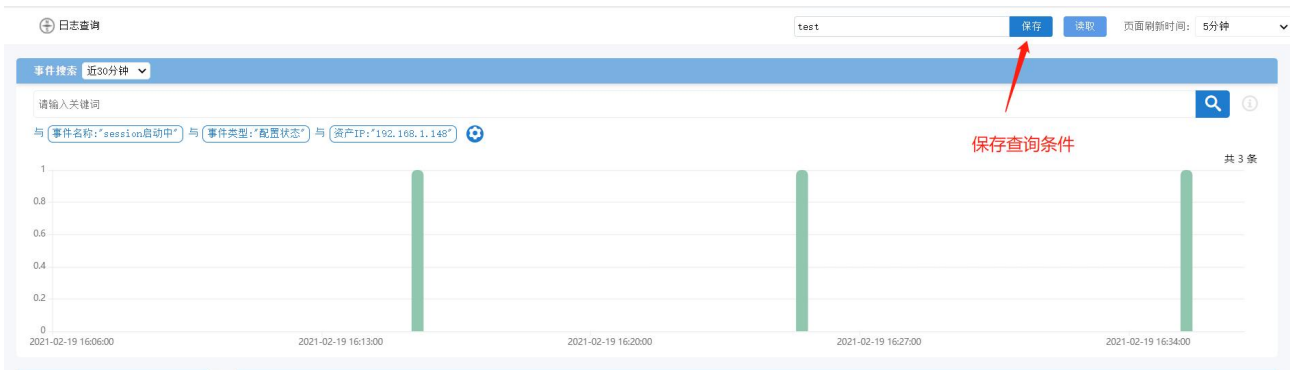


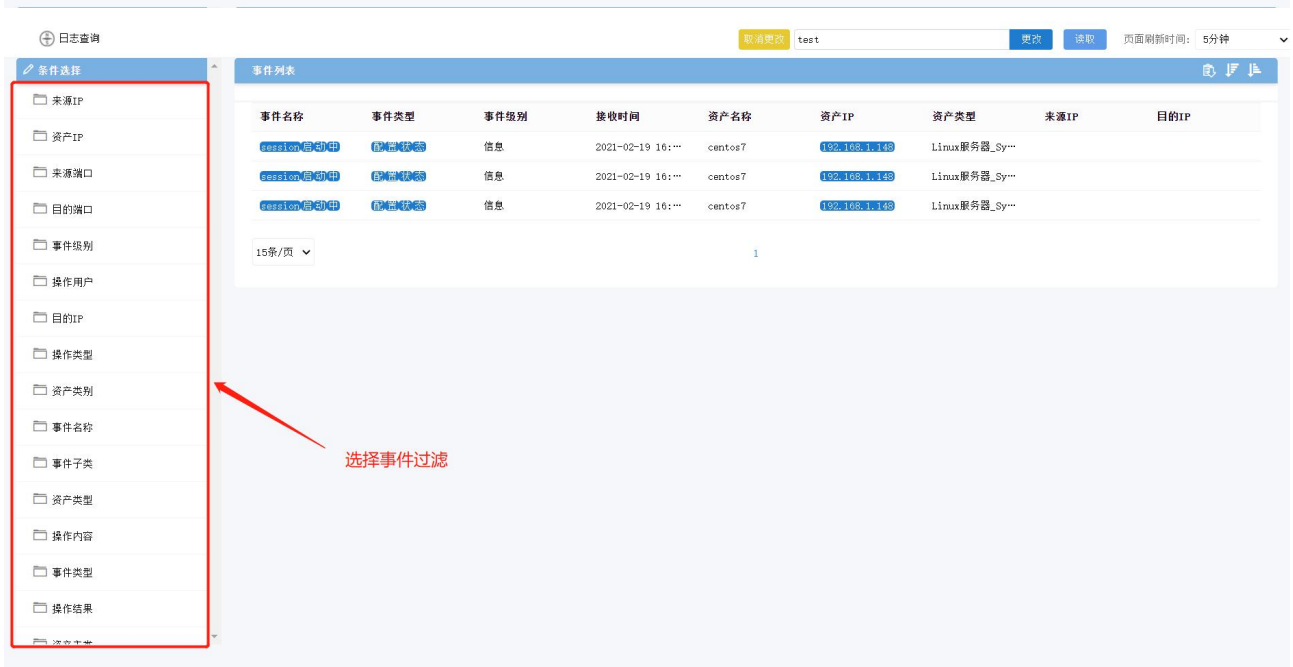
3.5 自定义图表查询统计条件

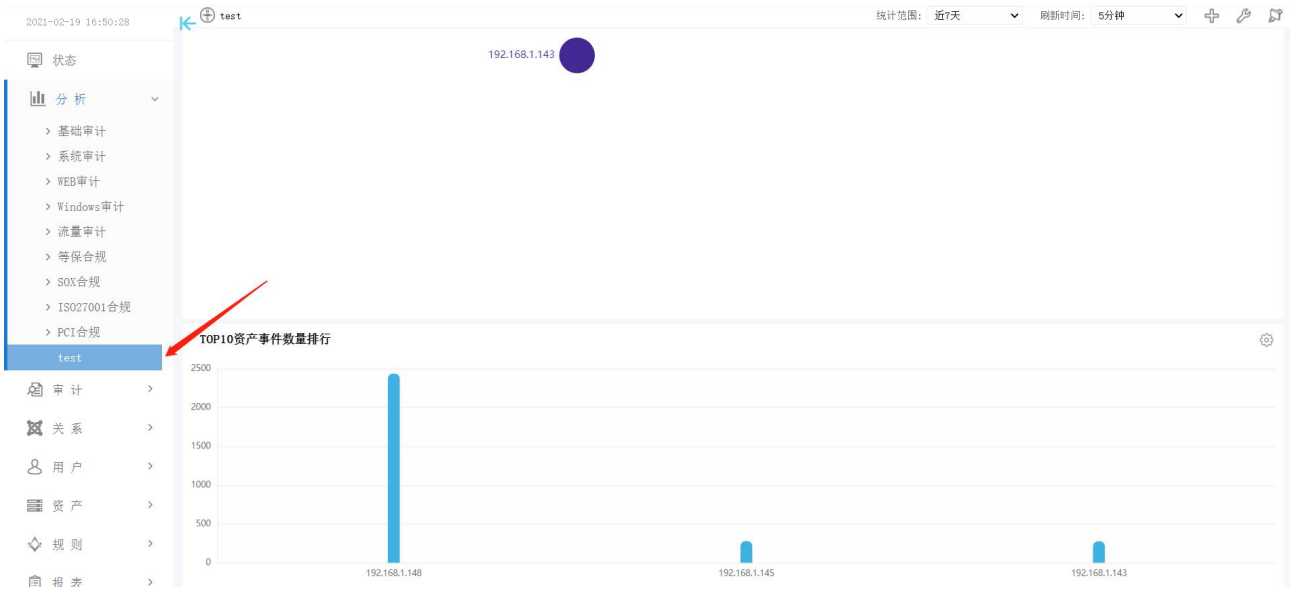
点击‘查看事件’自定义搜索条件，选择‘确定’跳转，可根据事件过滤条件和关键字等进行搜索，并将条件保存（需要添加查询条件名称）。再次进入自定义图表页面 ‘查询条件’项选择刚才添加的条件，可点击‘预览’查看图表，也可点击保存完成自定义图表查询统计条件的操作。

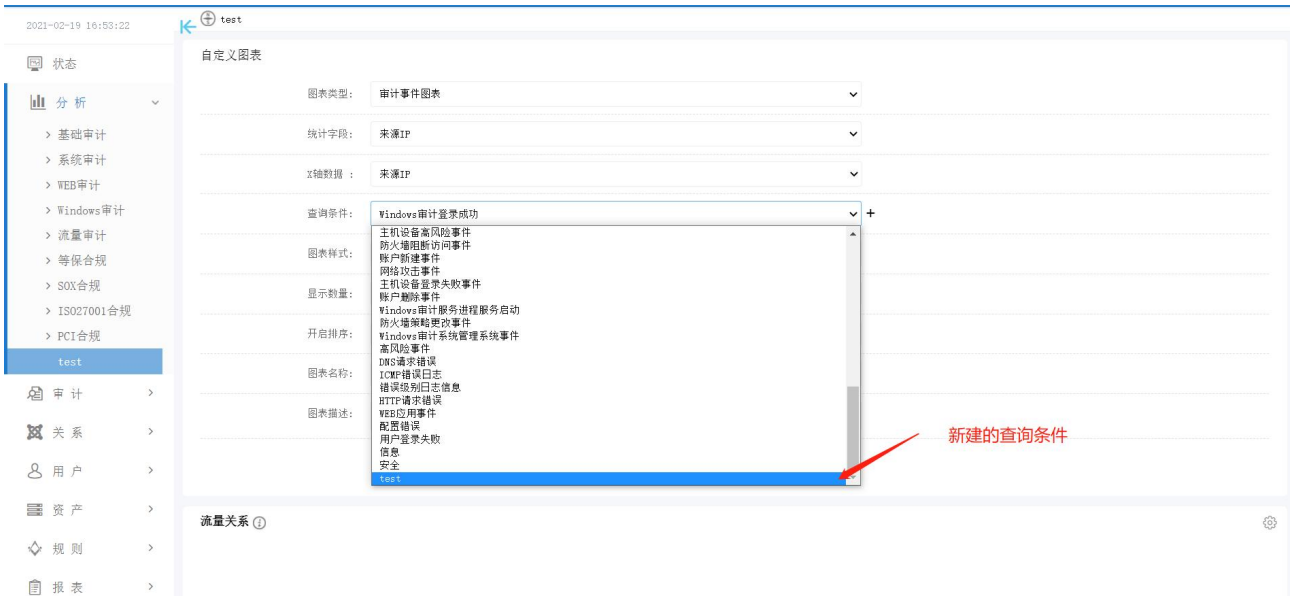



test
自定义图表
图表类型：
审计事件图表
统计字段：
来源IP
X轴数据：
来源IP
查询条件：
基础审计今日事件分析
图表样式：
柱状图
显示数量：
TOP5
开启排序：
关闭
图表名称：
请输入图表名称
图表描述：
请输入图表描述
保存创建
预览
取消
添加查询条件
跳转到查询条件添加页面
高等级事件按事件类型排行


日志查询
test
保存
读取
页面刷新时间：
5分钟
事件搜索
近30分钟
请输入关键词
保存查询条件
共 3 条
2021-02-19 16:06:00
2021-02-19 16:13:00
2021-02-19 16:20:00
2021-02-19 16:27:00
2021-02-19 16:34:00

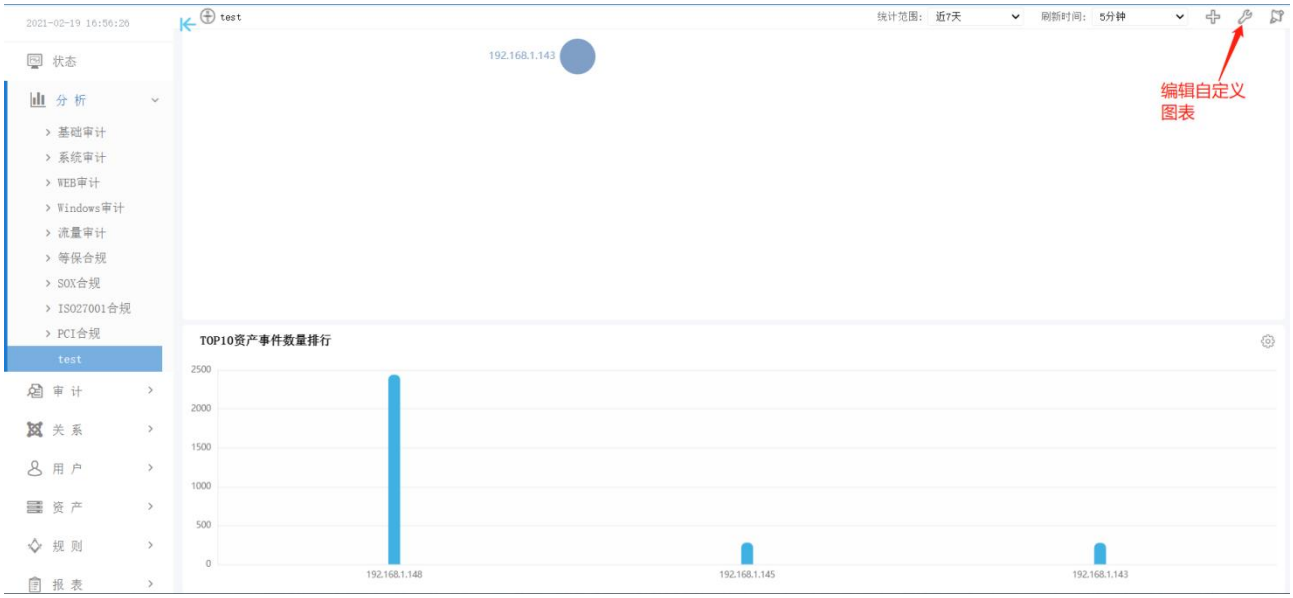

日志查询
取消更改
test
更改
读取
页面刷新时间：
5分钟
条件选择
来源IP
资产IP
来源端口
目的端口
事件级别
操作用户
目的IP
操作类型
资产类别
事件名称
事件子类
资产类型
操作内容
事件类型
操作结果
事件列表
事件名称
事件类型
事件级别
接收时间
资产名称
资产IP
资产类型
来源IP
目的IP
session启动中
配置状态
信息
2021-02-19 16:…
centos7
192.168.1.148
Linux服务器_Sy…
15条/页
选择事件过滤

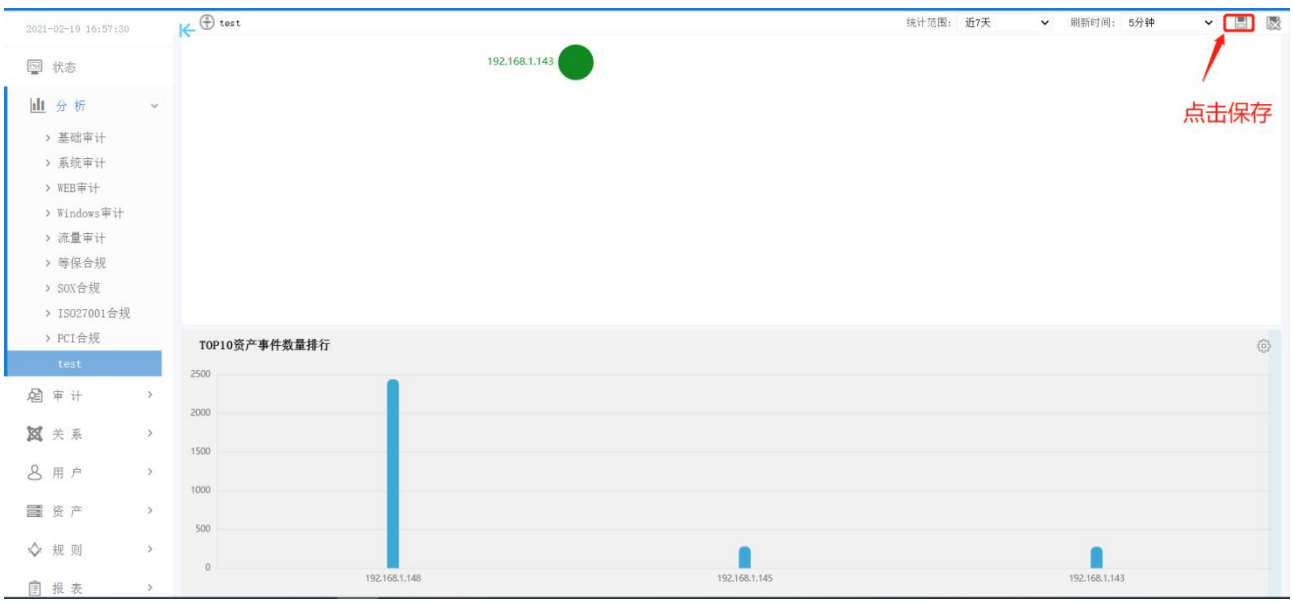




3.6 编辑自定义图表

进入图表可拖动状态→点击编辑图表→点击保存完成编辑自定义图表的操作。

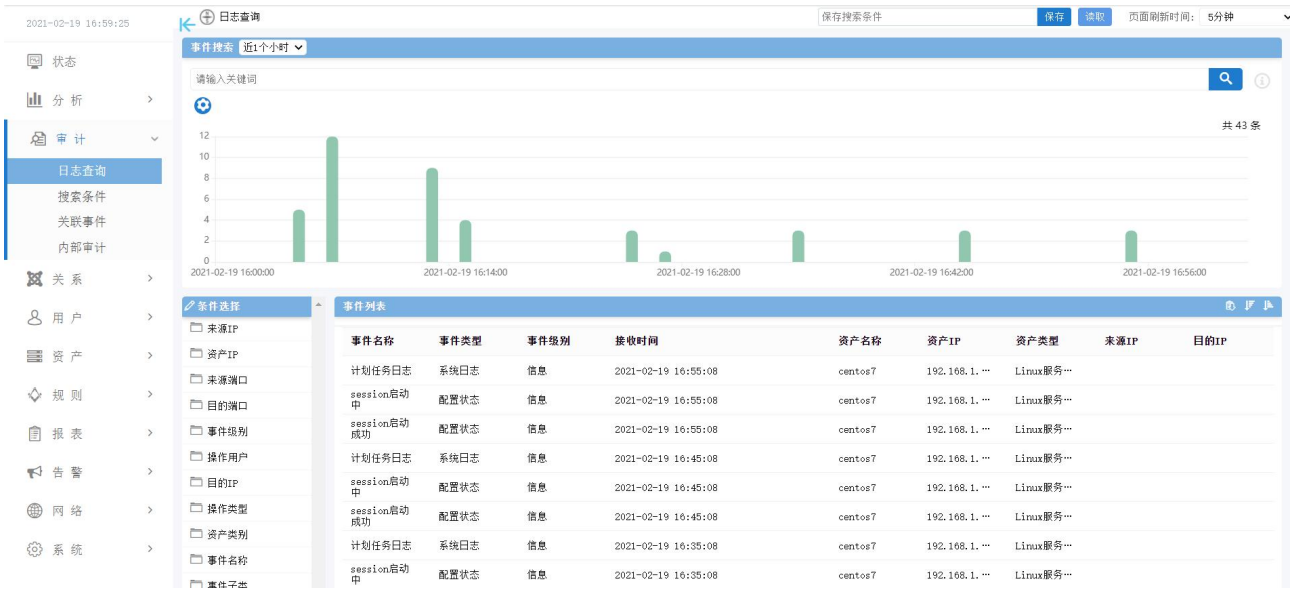

2021-02-19 16:56:26
test
统计范围: 近7天
刷新时间: 5分钟
状态
分 析
基础审计
系统审计
WEB审计
Windows审计
流量审计
等保合规
SOX合规
ISO27001合规
PCI合规
test
审 计
关 系
用 户
资 产
规 则
报 表
192.168.1.143
编辑自定义图表
TOP10资产事件数量排行
2500
2000
1500
1000
500
0
192.168.1.148
192.168.1.145
192.168.1.143


2021-02-19 16:57:30
test
统计范围: 近7天
刷新时间: 5分钟
状态
分 析
基础审计
系统审计
WEB审计
Windows审计
流量审计
等保合规
SOX合规
ISO27001合规
PCI合规
test
审 计
关 系
用 户
资 产
规 则
报 表
192.168.1.143
点击保存
TOP10资产事件数量排行
2500
2000
1500
1000
500
0
192.168.1.148
192.168.1.145
192.168.1.143

四. 审计

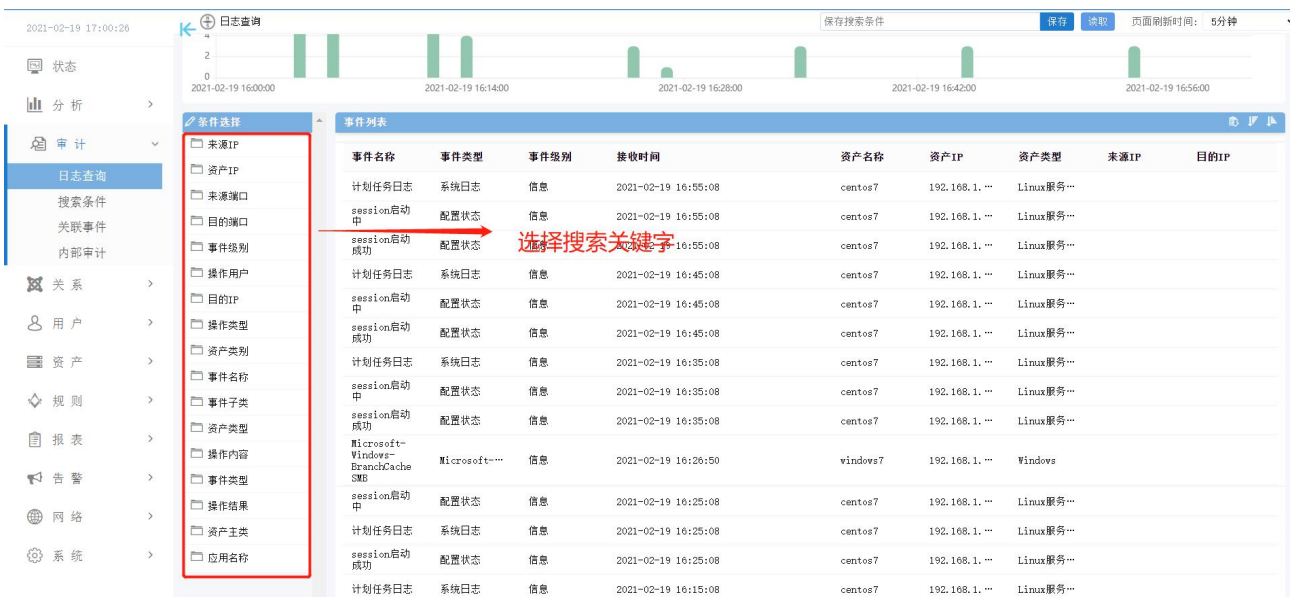
4.1 日志查询

菜单项‘审计’→‘日志查询’详情。

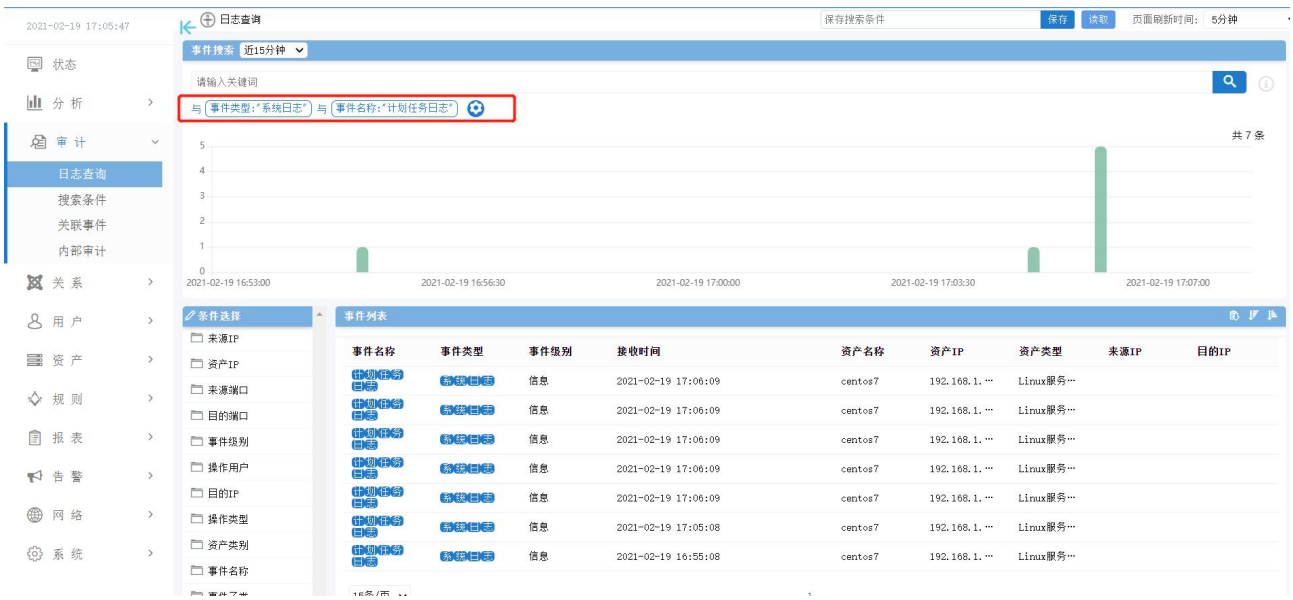


4.1.1 选择过滤关键字

按条件过滤事件

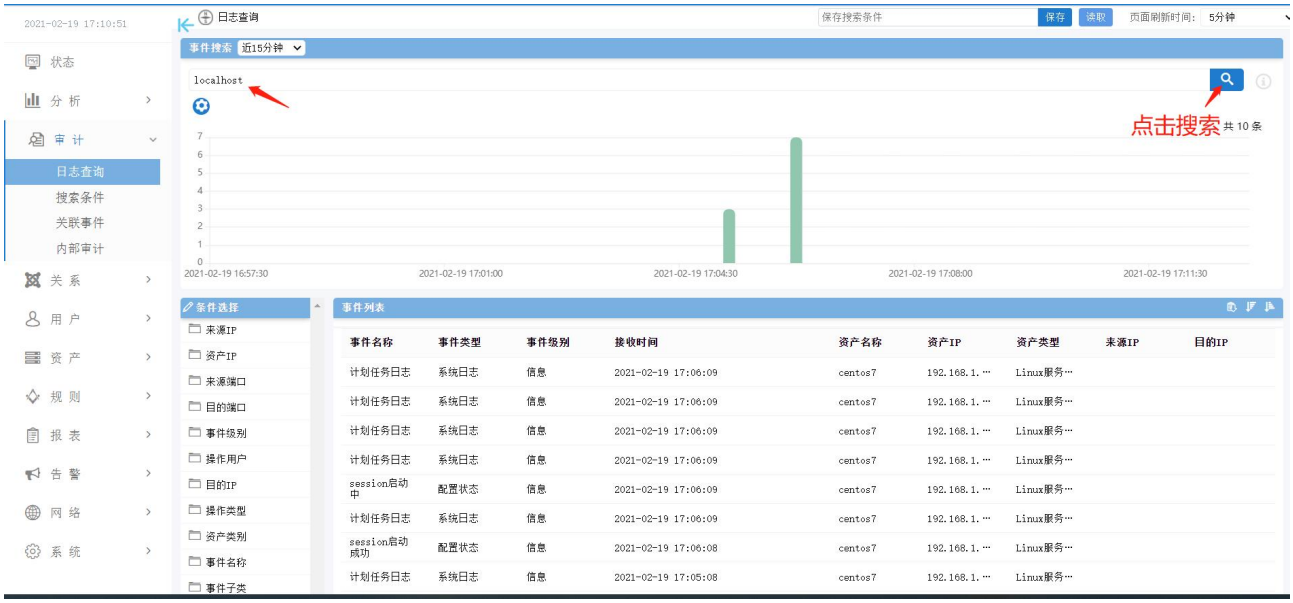


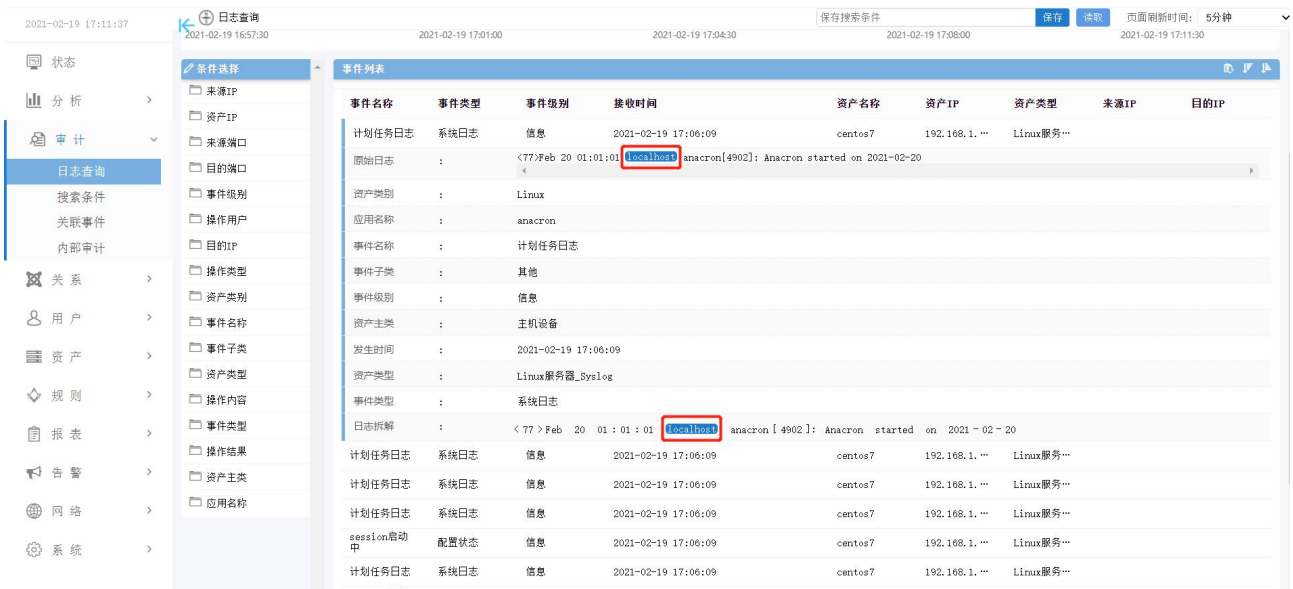
点击已选择的条件可删除该条件的限制。



4.1.2 全文搜索

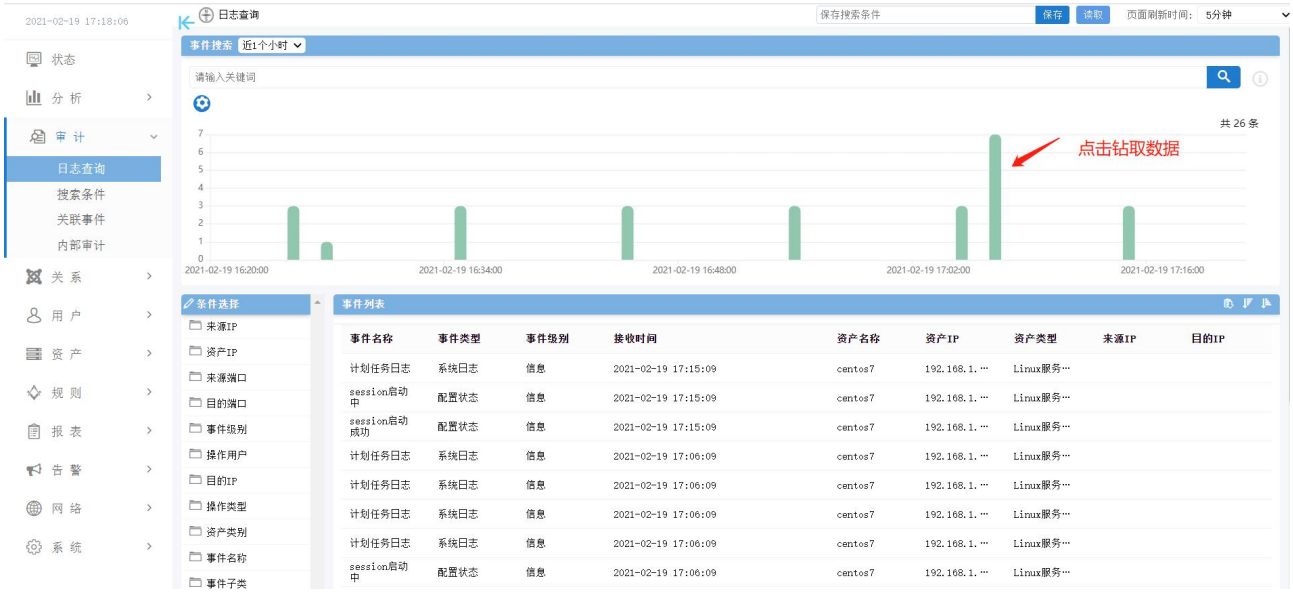
在事件搜索输入框内输入关键字，可查询包含关键字内容的事件，搜索结果中关键字高亮蓝色背景显示。支持多个关键字搜索，多个关键字用‘|’分割。

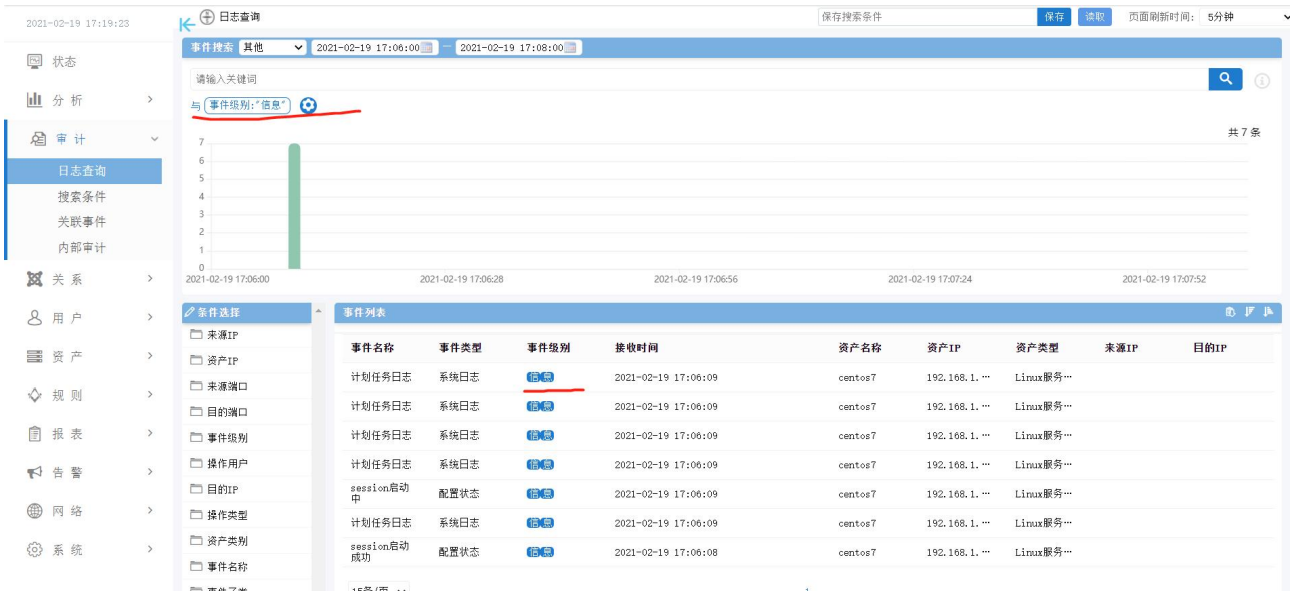




4.1.3 钻取关联数据

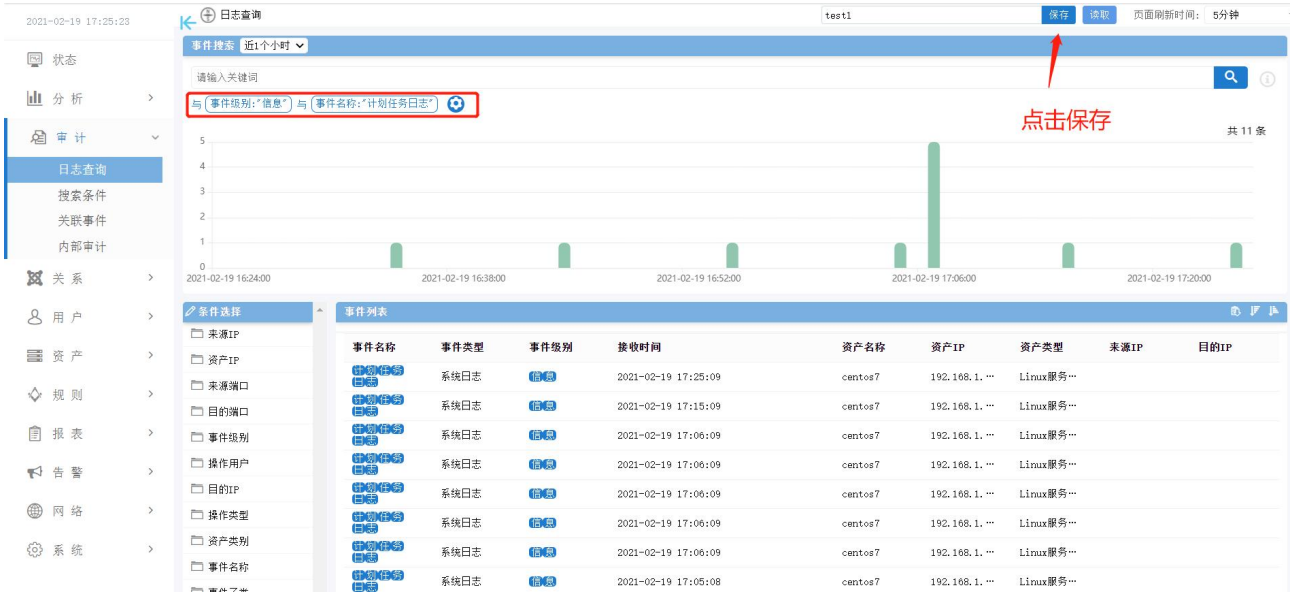
点击图表的数据柱可查看该数据柱所表示的条件在一定时间范围内的数据详情。

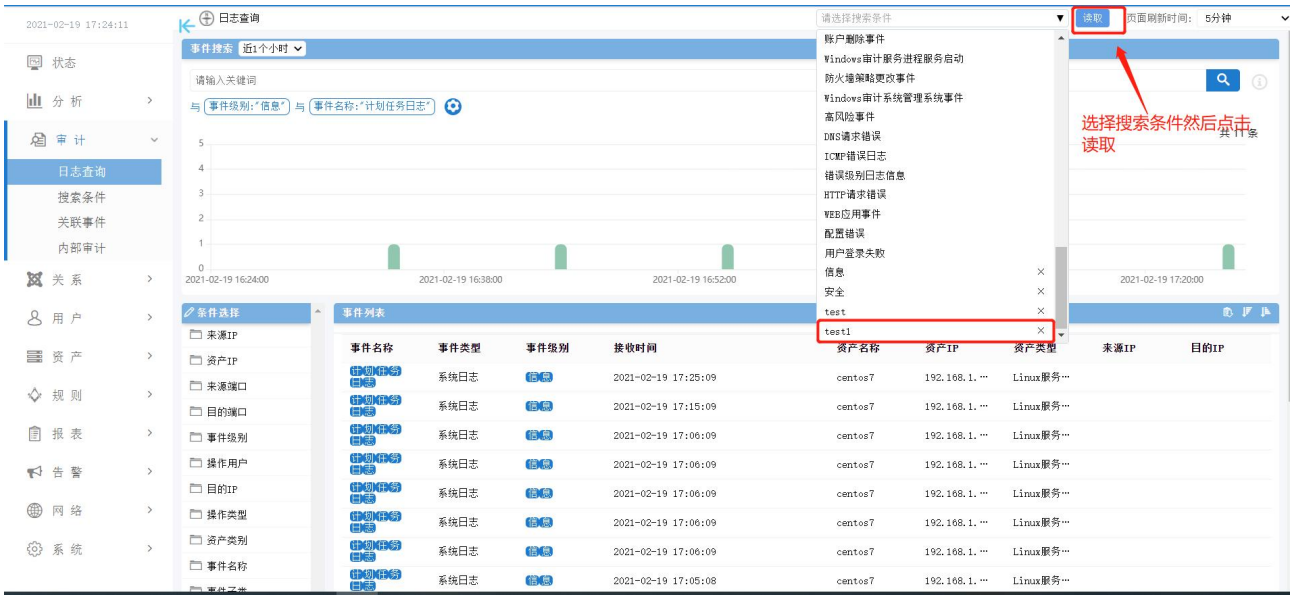




4.1.4 保存查询条件

搜索结果所对应的条件可在页面右上角‘保存’左侧的输入框内命名，点击‘保存’可将该搜索条件保存，方便快捷查询。



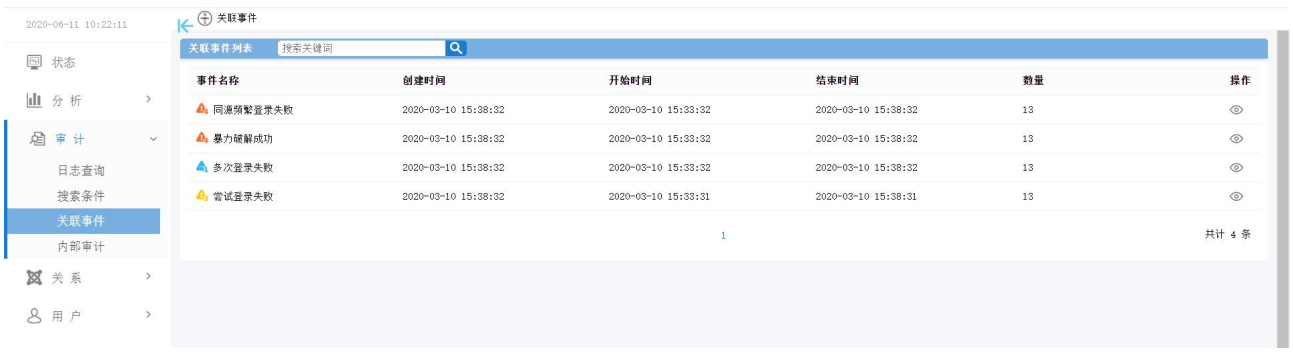


4.1.5 原始日志

查看原始日志：菜单项‘审计’→‘日志查询’→‘日志拆解’。

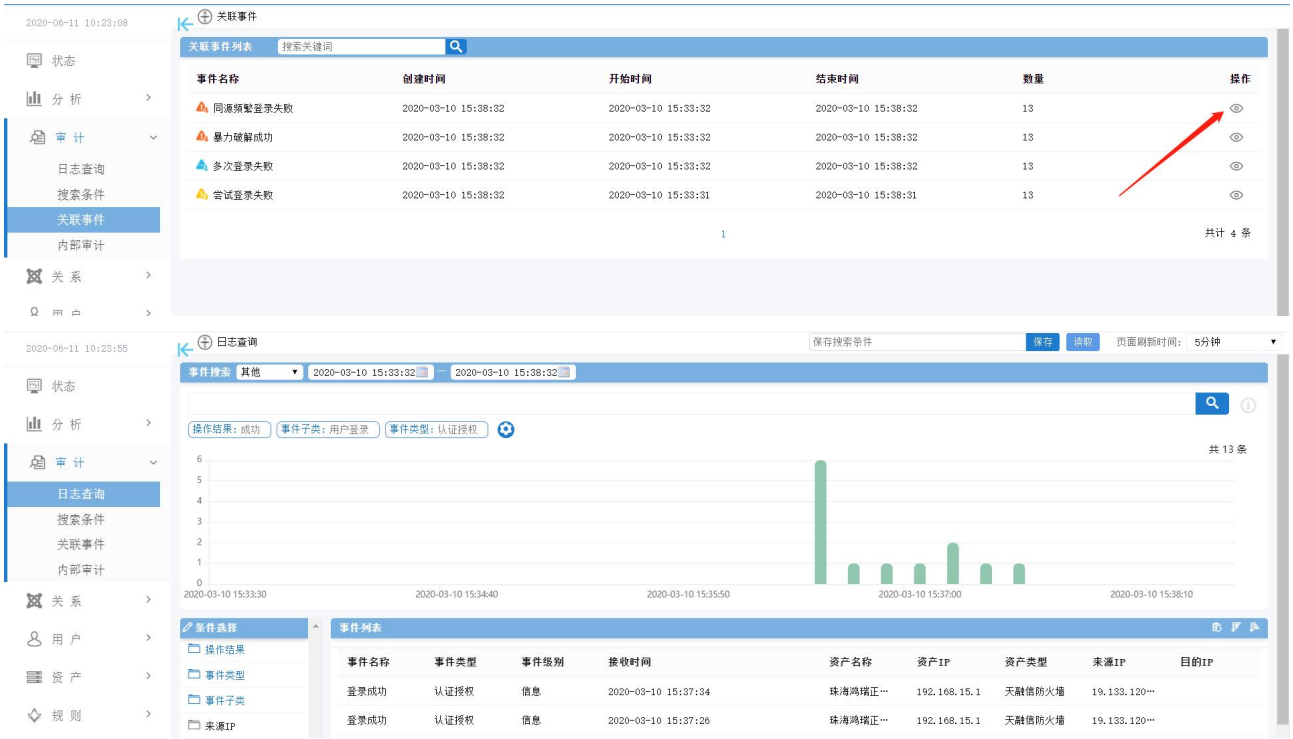
4.2 关联事件

查看关联事件：菜单项‘审计’→‘关联事件’。



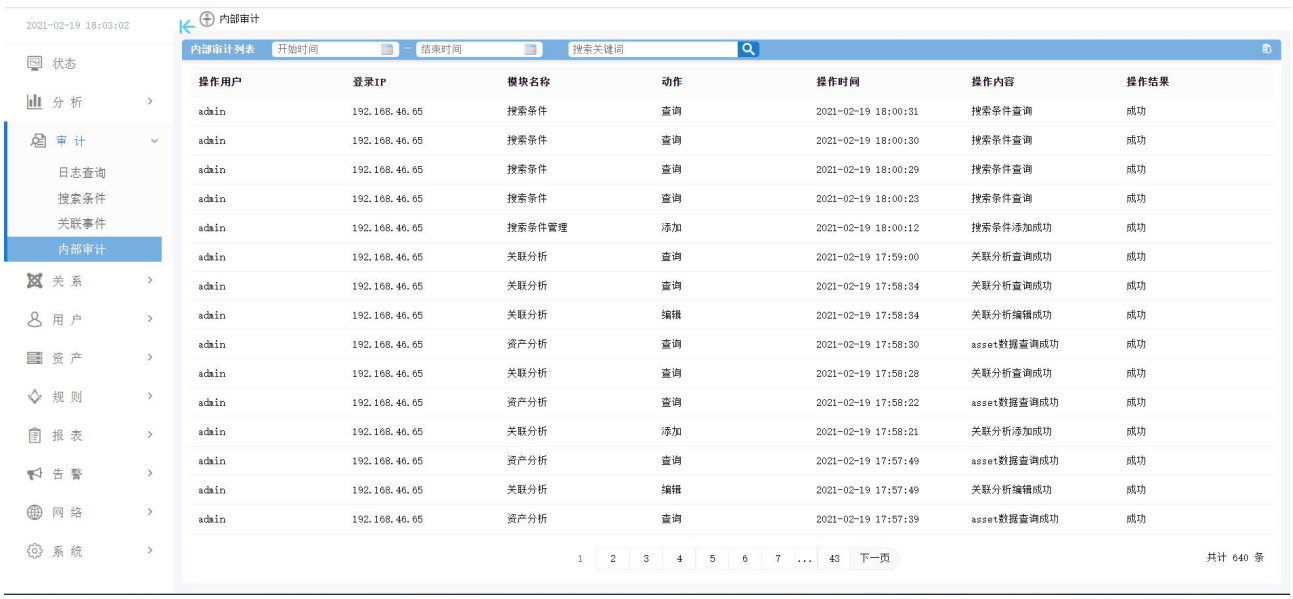
4.2.1 钻取关联事件

点击关联事件列表左侧‘查看’图表，可查看该关联事件的详情。



4.3 内部审计

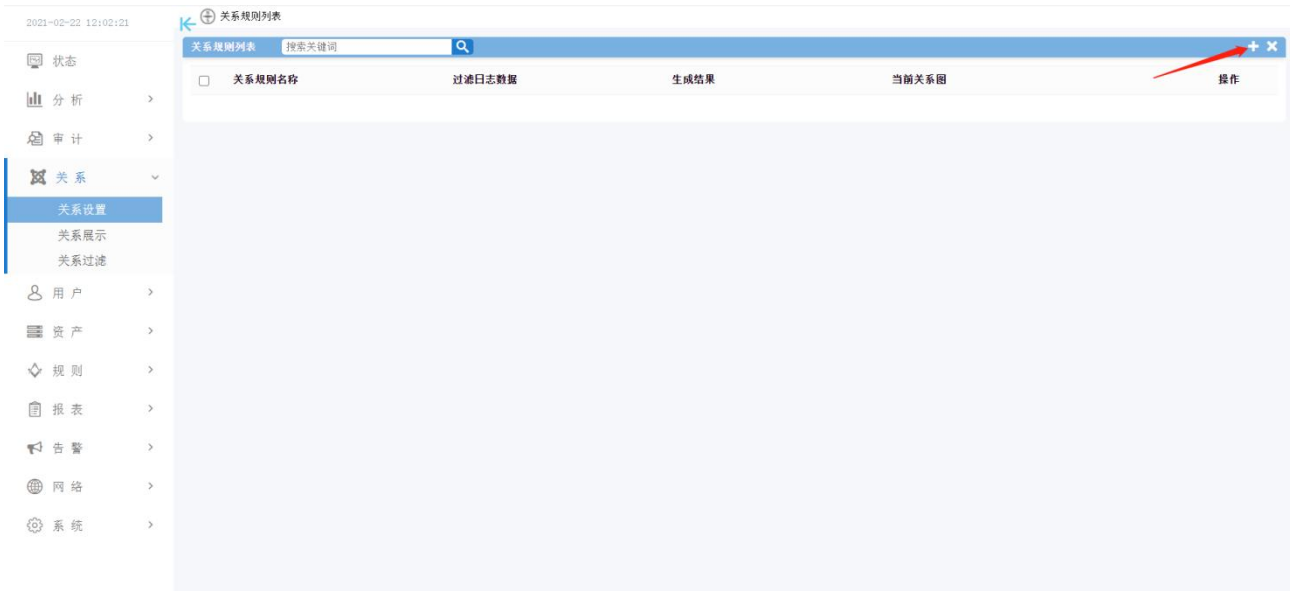
查看和检索内部审计事件：菜单项‘审计’→‘内部审计’。



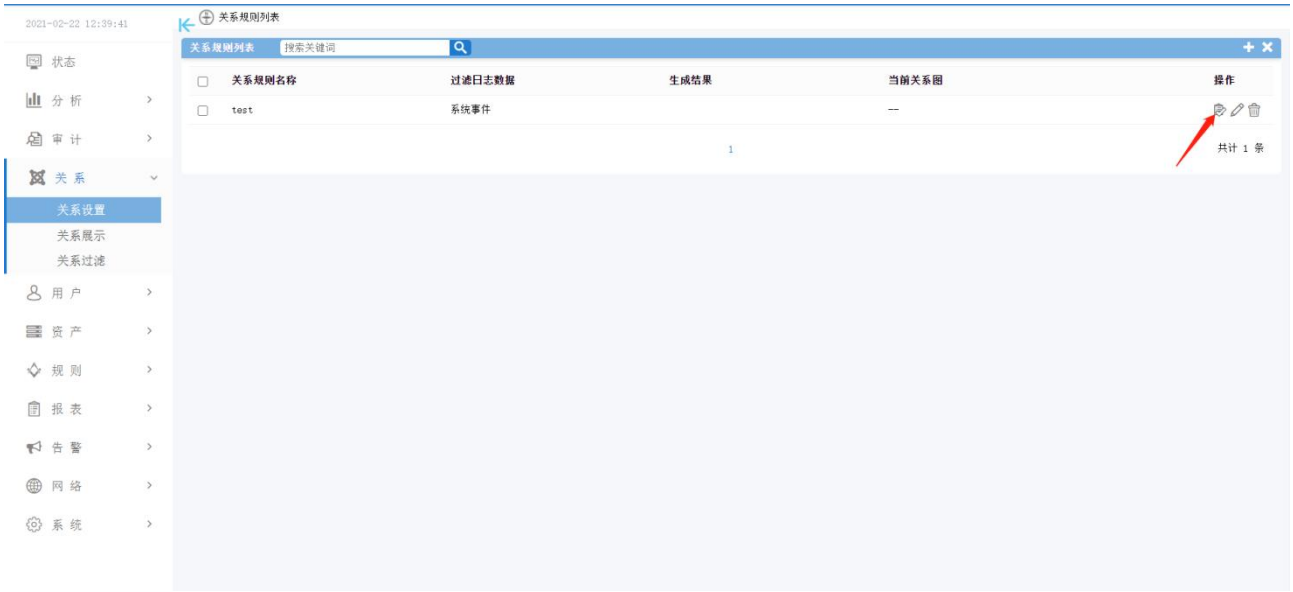
五. 关系

5.1 关系设置

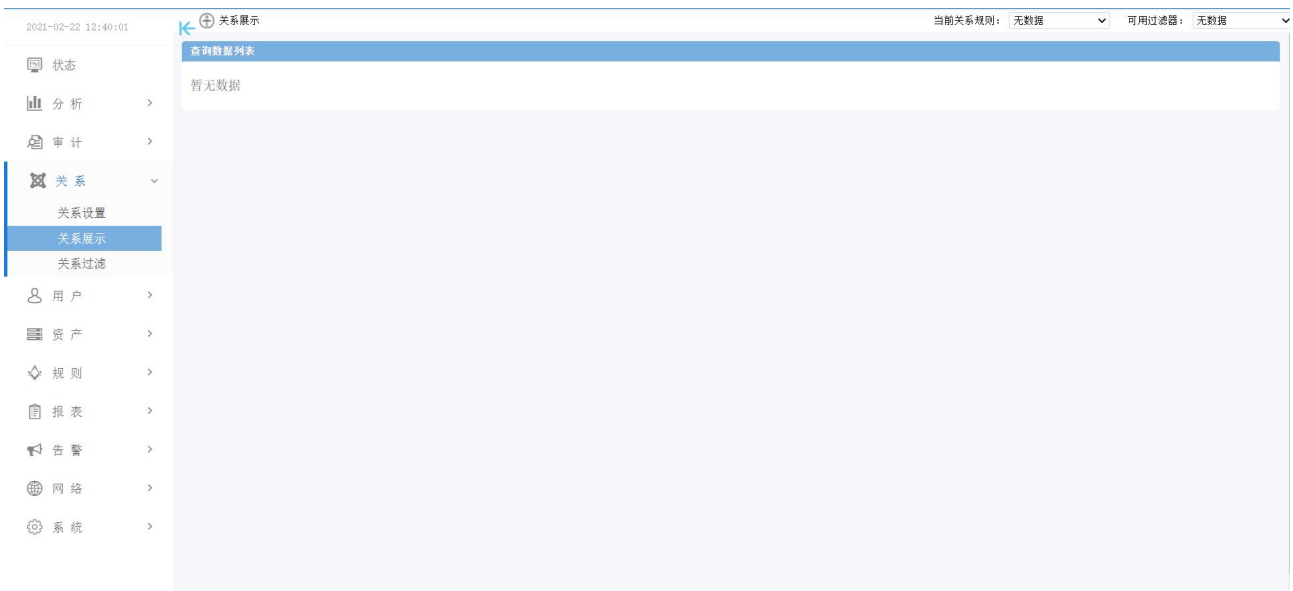
5.1.1 添加关系设置



5.1.2 生成关系图

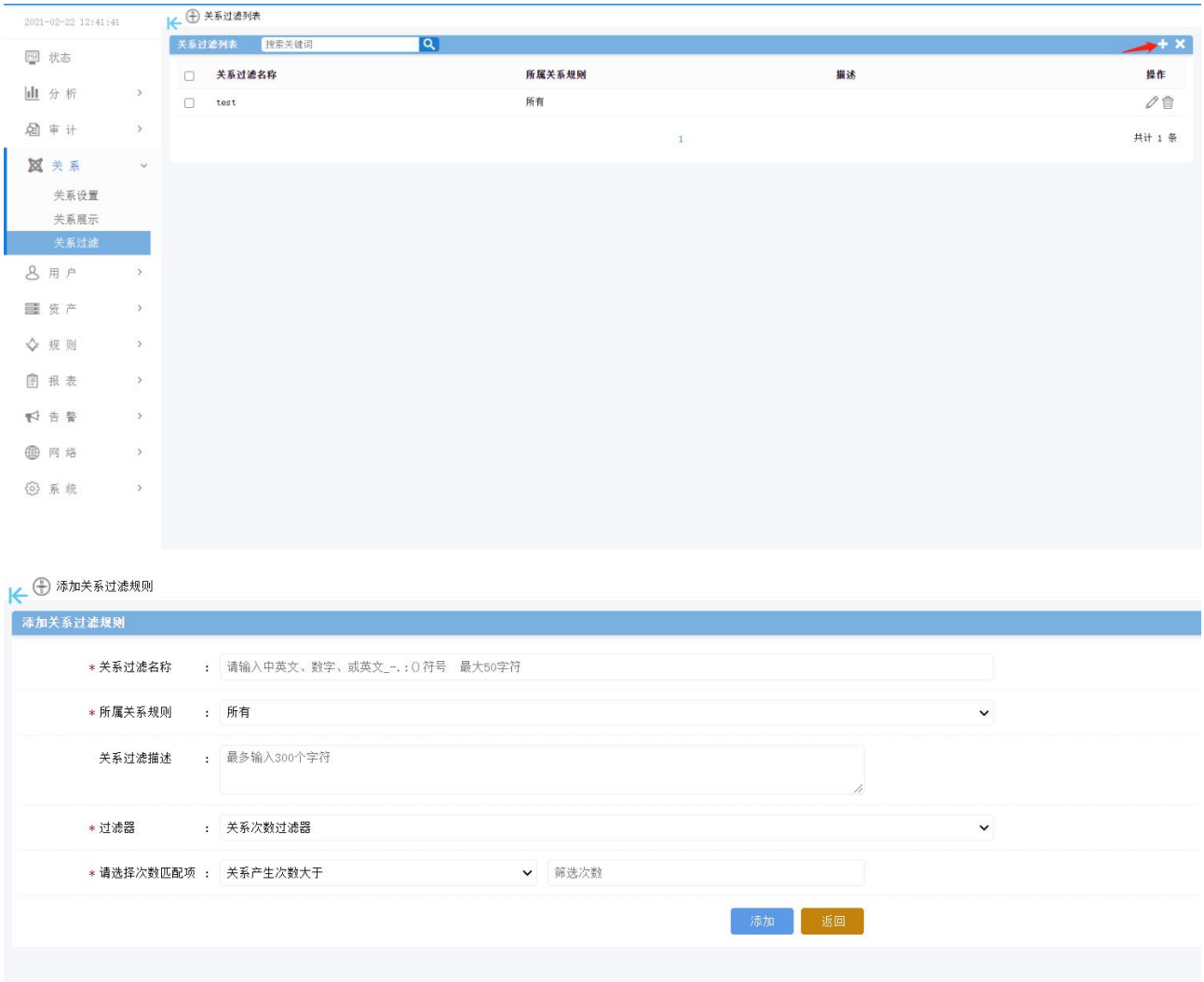


5.2 关系展示

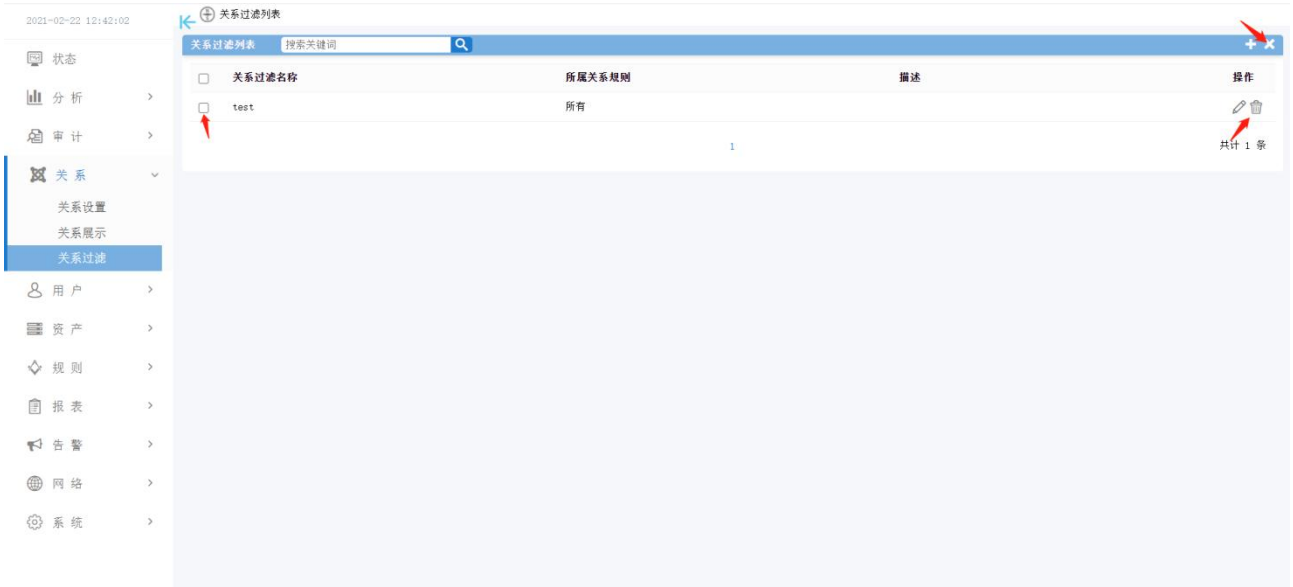


5.3 关系过滤

5.3.1 添加关系过滤



5.3.2 删除关系过滤


2021-02-22 12:42:02
状态
分 析
审 计
关 系
关系设置
关系展示
关系过滤
用 户
资 产
规 则
报 表
告 警
网 络
系 统
关系过滤列表
关系过滤列表
搜索关键词
关系过滤名称
所属关系规则
描述
操作
test
所有
共计 1 条

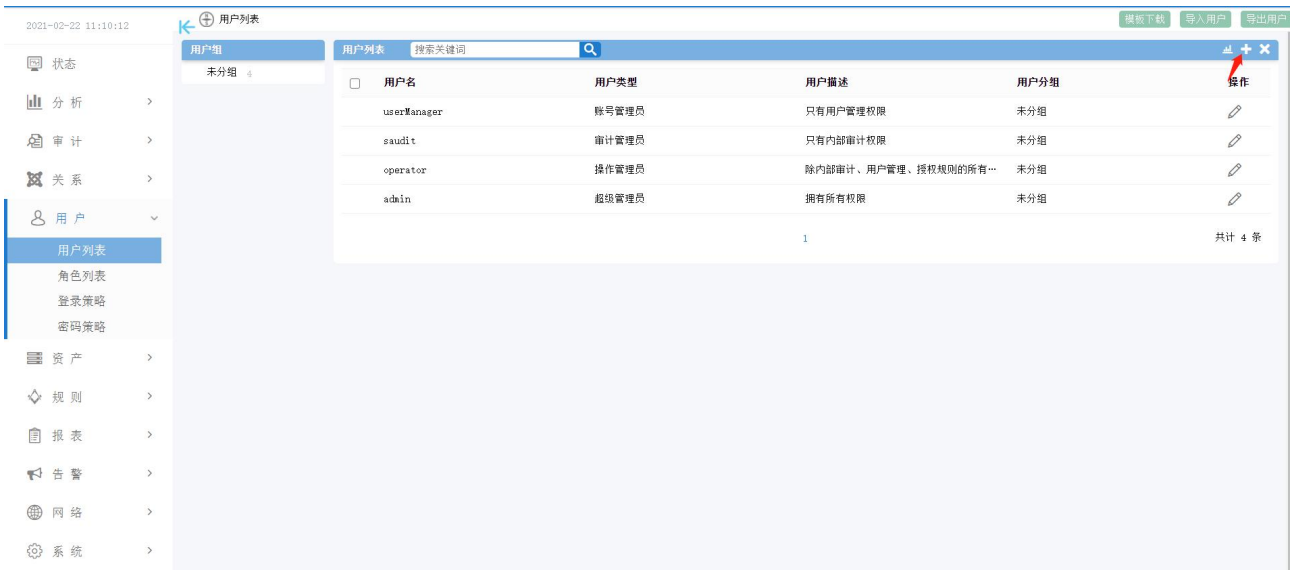
六. 用户

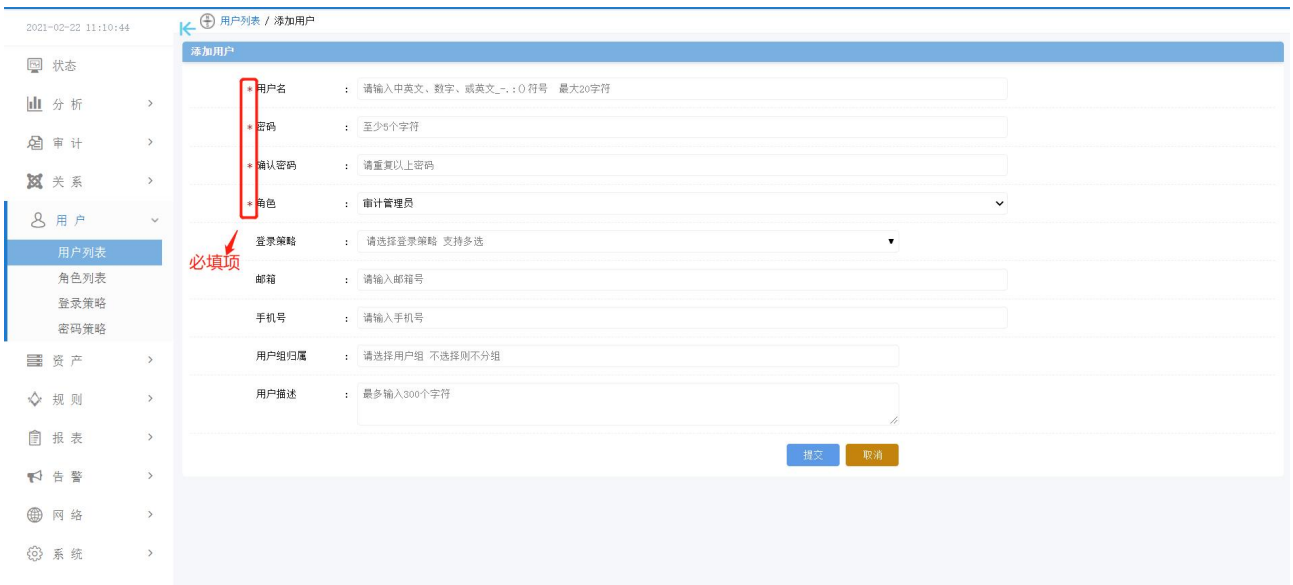
6.1 用户列表

6.1.1 添加用户

点击右上角‘添加图标’，进入添加资产界面

将添加用户各项信息填完点击提交即可。

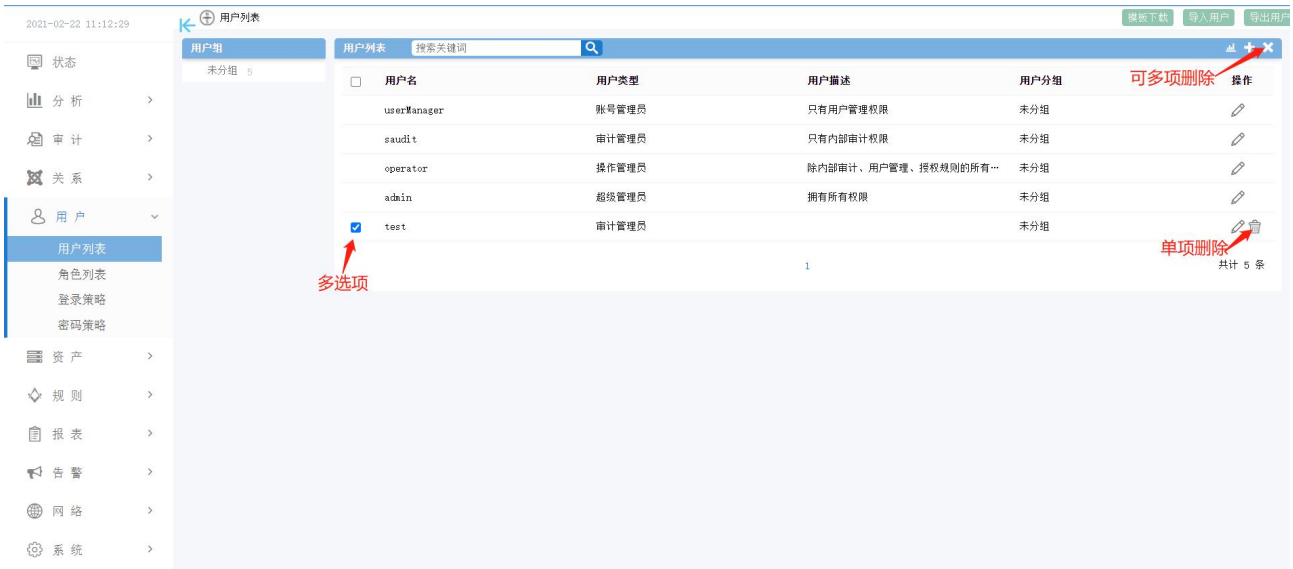




6.1.2 删除用户

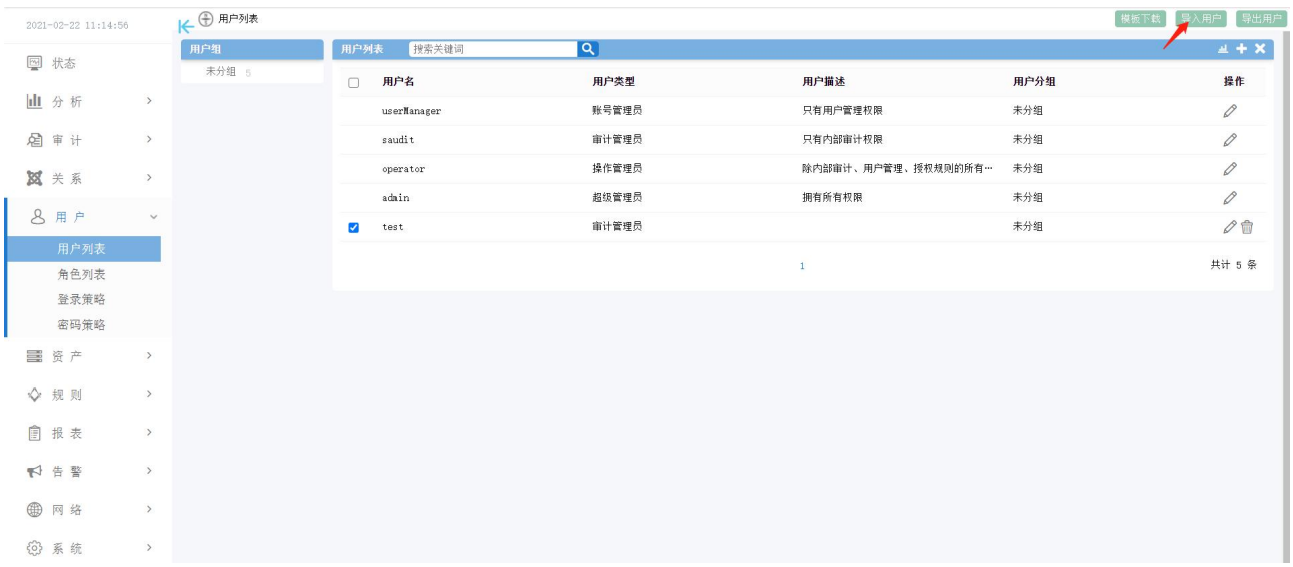
点击用户列表左边方框可进行多选用户，然后点击右上角‘删除’图表进行多项删除。

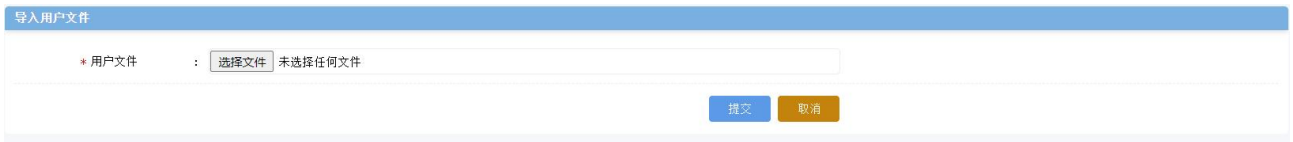
点击用户列表右边的‘删除’图标（垃圾桶），可以进行单项删除。



6.1.3 导入用户

点击右上角‘导入用户’模块，可进行用户导入。（注：导入文件必须是 xlsx 文件）



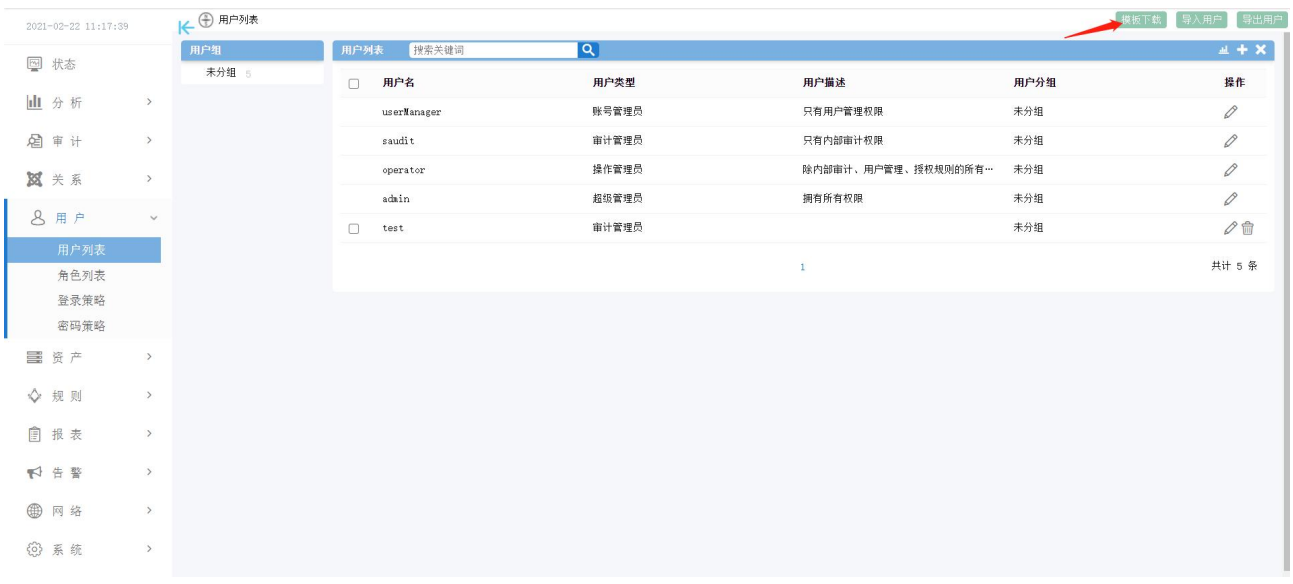


6.1.4 导出用户

点击右上角‘导出用户’功能，可以进行导出用户，对系统用户进行备份。

6.1.5 模板下载

点击右上角‘模板下载’功能，直接下载‘用户模板 xlsx’文件。



6.2 角色列表

菜单项‘用户’→‘角色列表’子项。进入角色列表展示页面。

6.2.1 添加角色

点击角色列表右上角‘添加’图标，进入添加角色界面，按要求填写和选择相应的添加项→点击‘提交’完成添加角色的操作。

6.2.2 删除角色

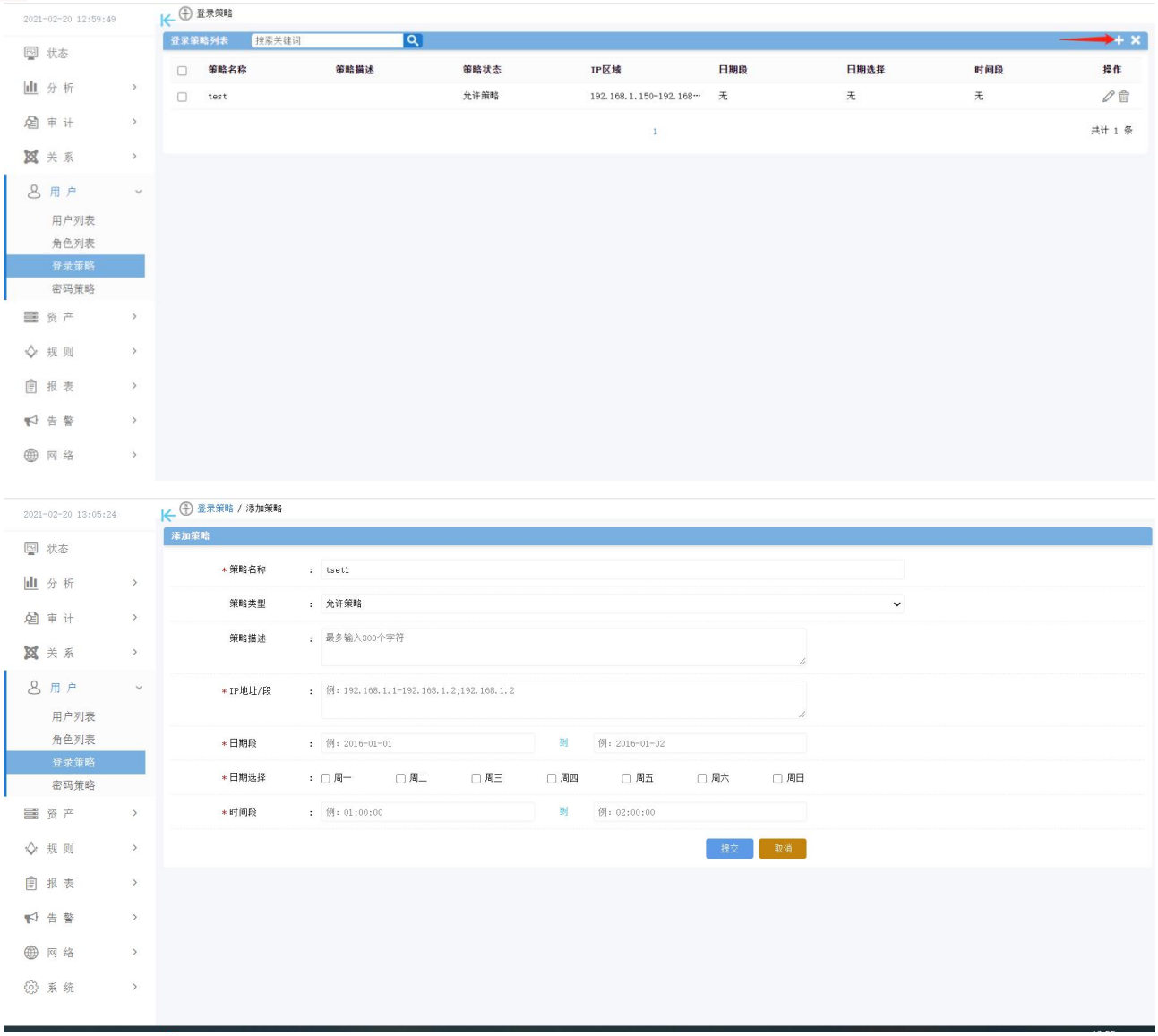
点击角色列表标题行左侧的复选框，可选中该页所有角色，点击每条角色信息左侧的复

选框则可选中该条角色信息→点击角色列表右上角‘删除’按钮，系统提示：确定删除所选项吗？点击‘确定’，完成批量删除角色的操作。点击每条角色信息‘操作’列‘删除’图标，系统提示：确定删除此项吗？点击‘确定’，完成删除角色的操作。系统内置的角色不支持删除。

6.3 登录策略

6.3.1 添加登陆策略

点击登录策略列表右上角‘添加’图标，进入添加登录策略界面，按要求填写和选择相应的添加项→点击‘提交’完成添加登录策略的操作。

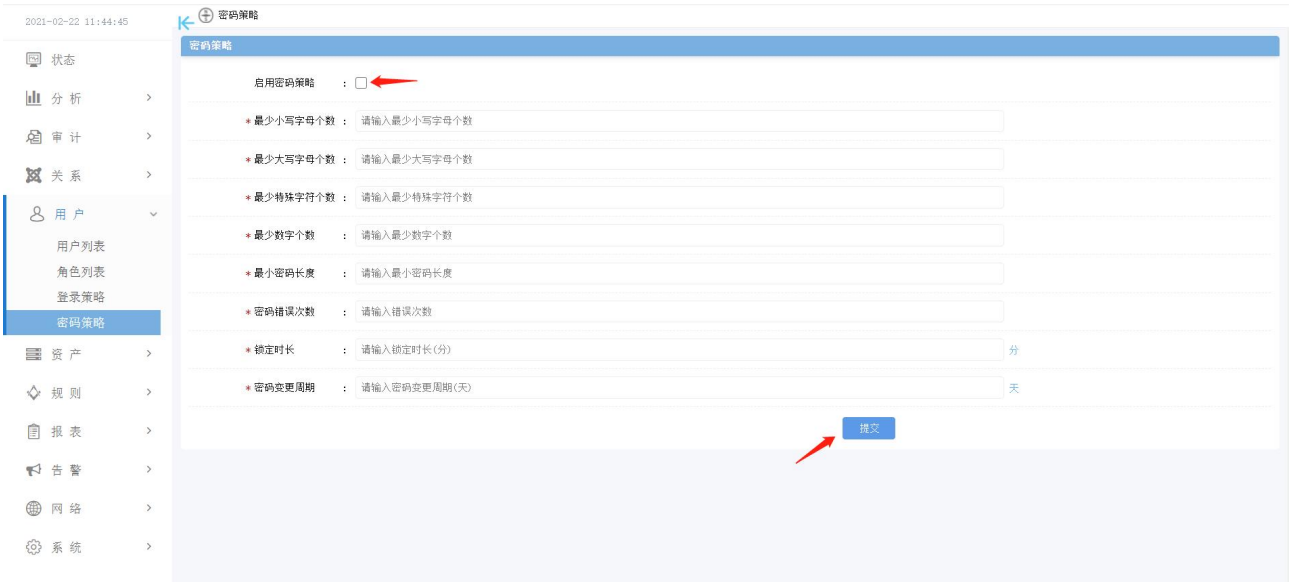


6.3.2 删除登陆策略

点击登录策略列表标题行左侧的复选框，可选中该页所有登录策略，点击每条登录策略左侧的复选框则可选中该条登录策略→点击登录策略列表右上角‘删除’按钮，系统提示：确定删除所选项吗？点击‘确定’，完成批量删除登录策略的操作。点击每条登录策略‘操作’列‘删除’图标，系统提示：确定删除此项吗？点击‘确定’，完成删除登录策略的操作。

6.4 密码策略

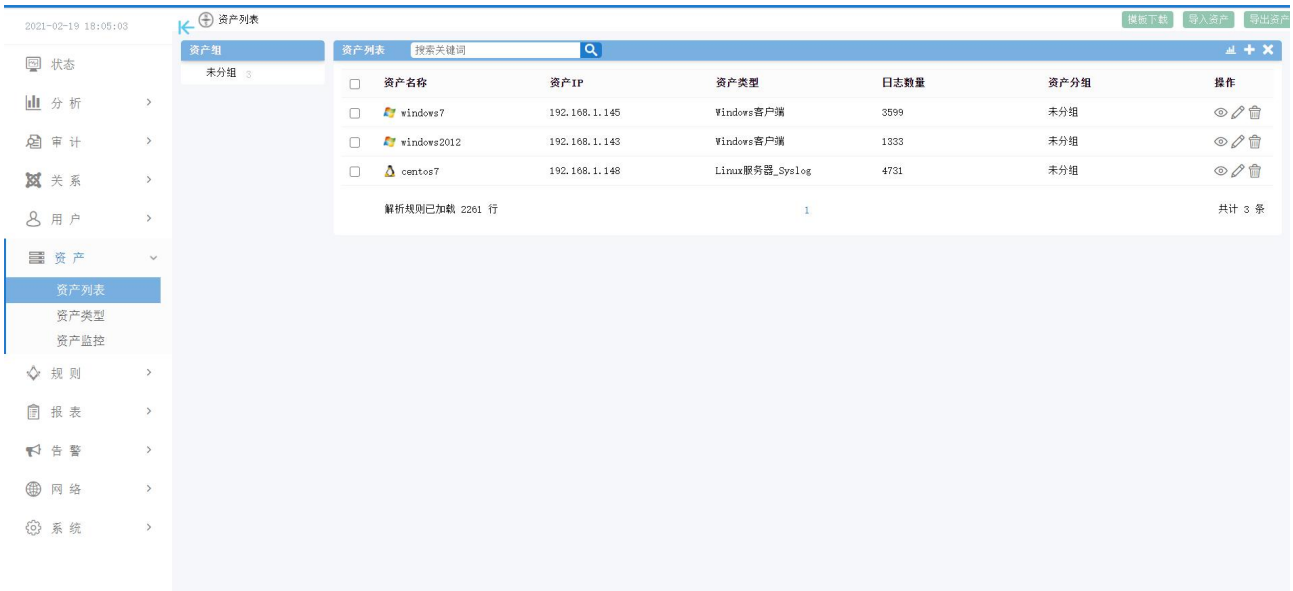
根据需求将密码策略各项设置填好，然后点击启用密码策略，点击提交。



七. 资产

7.1 资产列表

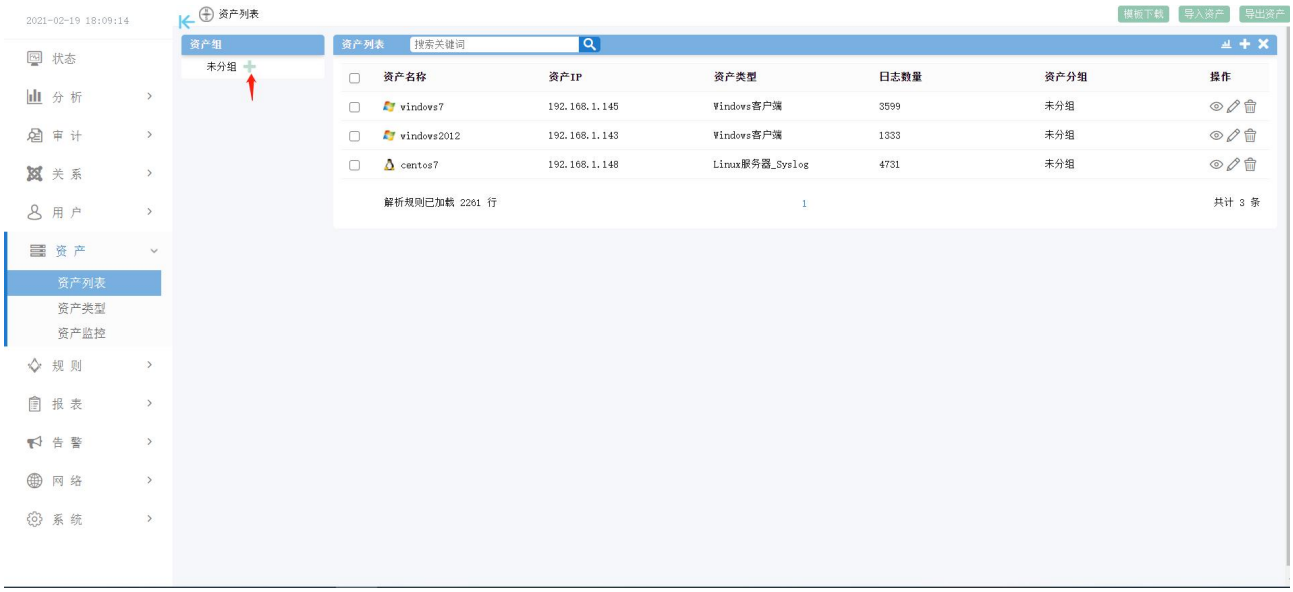
查看资产列表：菜单项‘资产’→‘资产列表’。

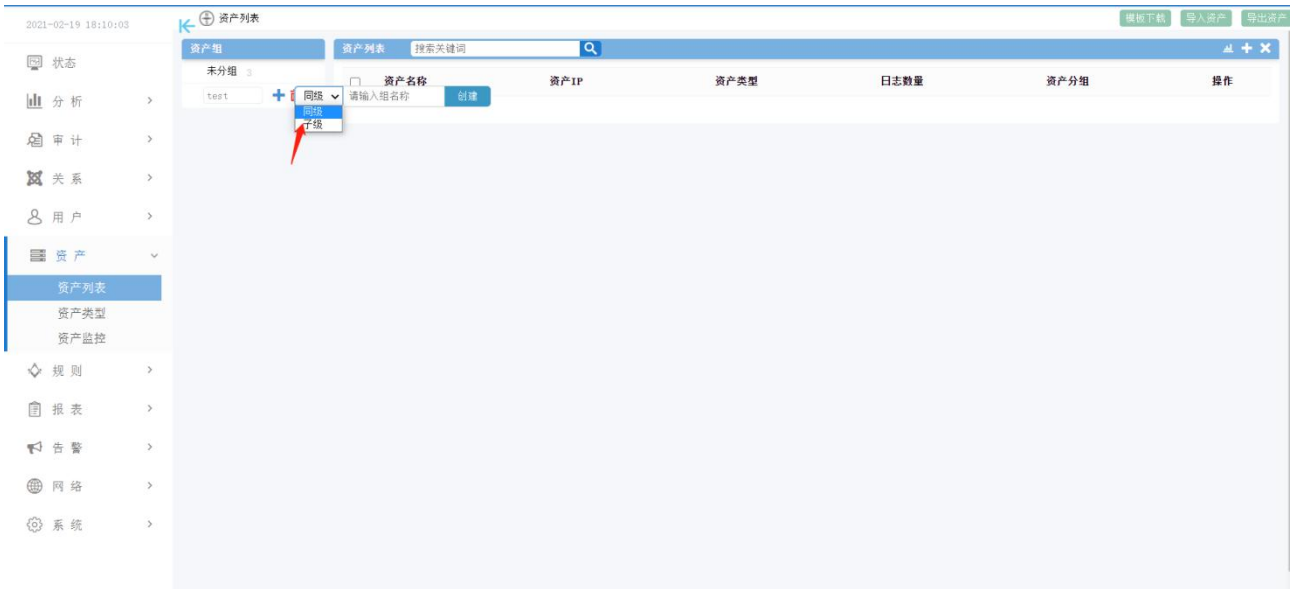


7.1.1 资产组管理

7.1.1.1 编辑资产组

点击左侧资产组列表的‘编辑组’图标→显示资产组编辑界面，可根据需要进行添加同级，添加下级，删除，修改资产组操作，点击‘提交’完成编辑资产组操作。

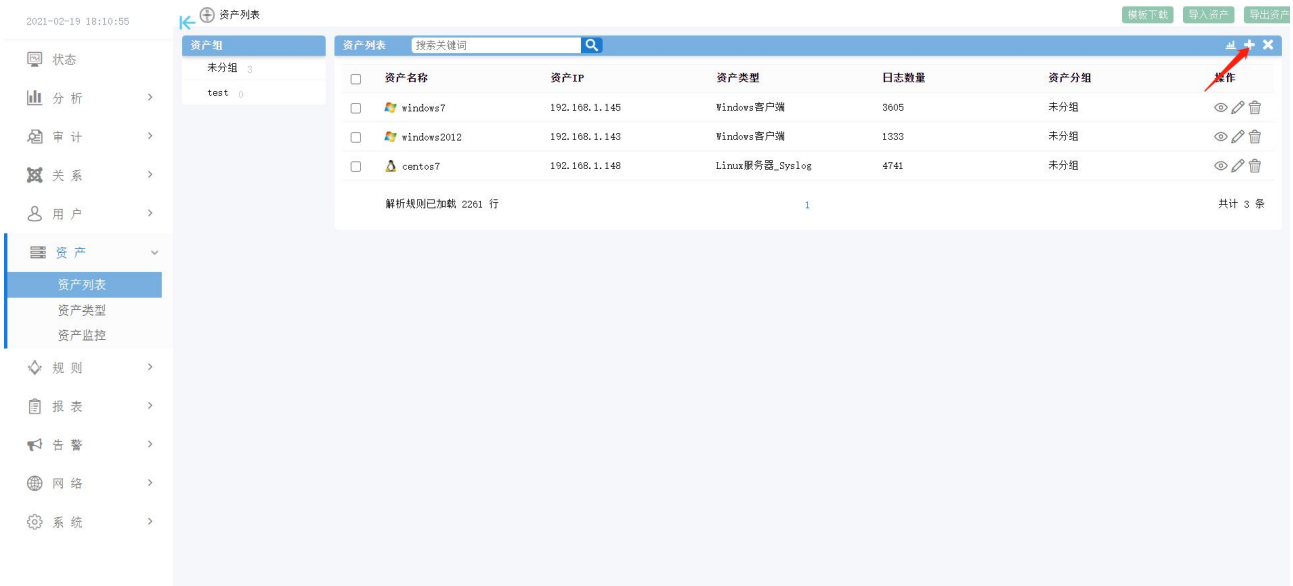




7.1.2 资产添加/编辑

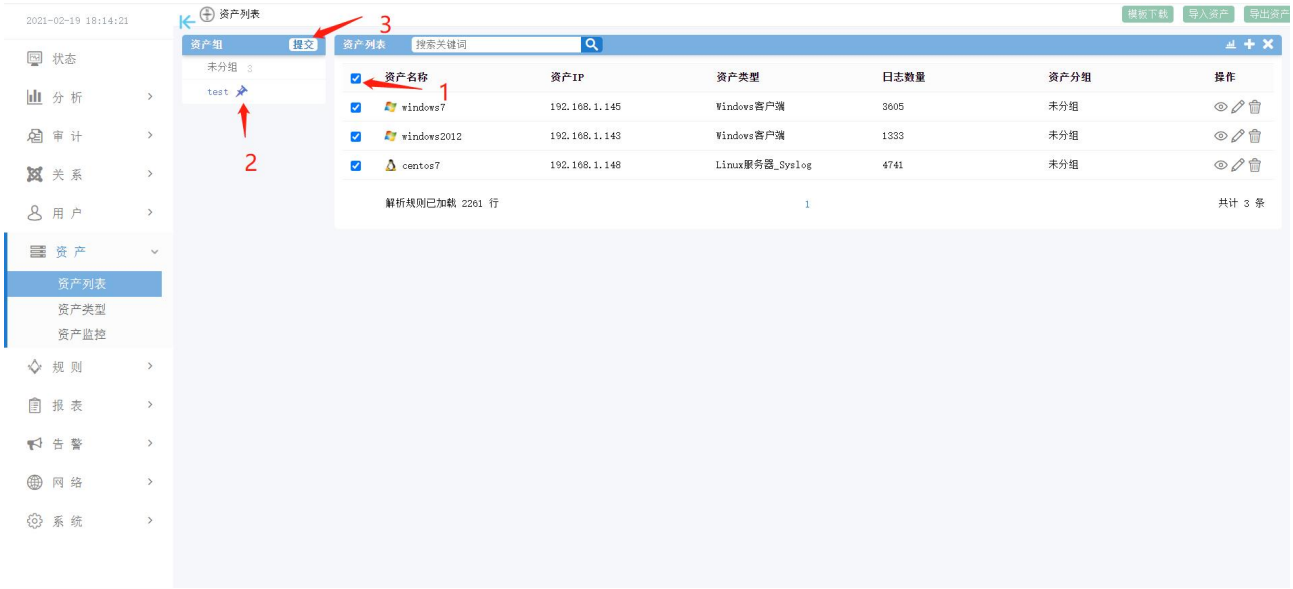
点击资产列表上方‘添加’图标，进入添加资产界面。

点击每条资产信息‘操作’列中的‘编辑’图标，进入编辑资产界面，可根据需要对需要修改的项进行编辑，点击提交完成资产编辑操作。



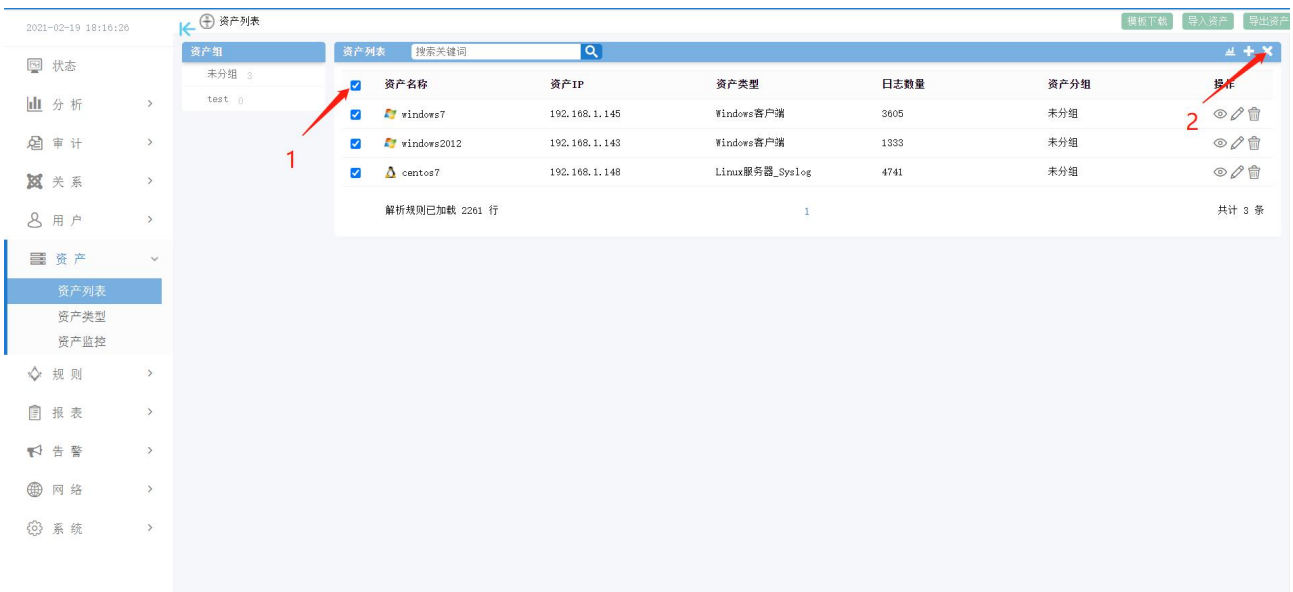
7.1.3 批量修改资产组

点击资产列表标题行左侧的复选框，可选中该页所有资产，点击每条资产信息左侧的复选框则选中该条资产→选择想要分组的资产组名→点击添加按钮，完成批量修改资产组操作。



7.1.4 批量删除资产

点击资产列表标题行左侧的复选框，可选中该页所有资产，点击每条资产信息左侧的复选框则选中该条资产→点击资产列表右上角删除按钮，系统提示：确定删除所选项吗？点击确定，完成批量删除资产的操作。



7.1.5 模板下载

点击系统右上角‘模板下载’按钮，即可下载资产模板。

7.1.6 批量导入资产

7.1.7 导出所有资产

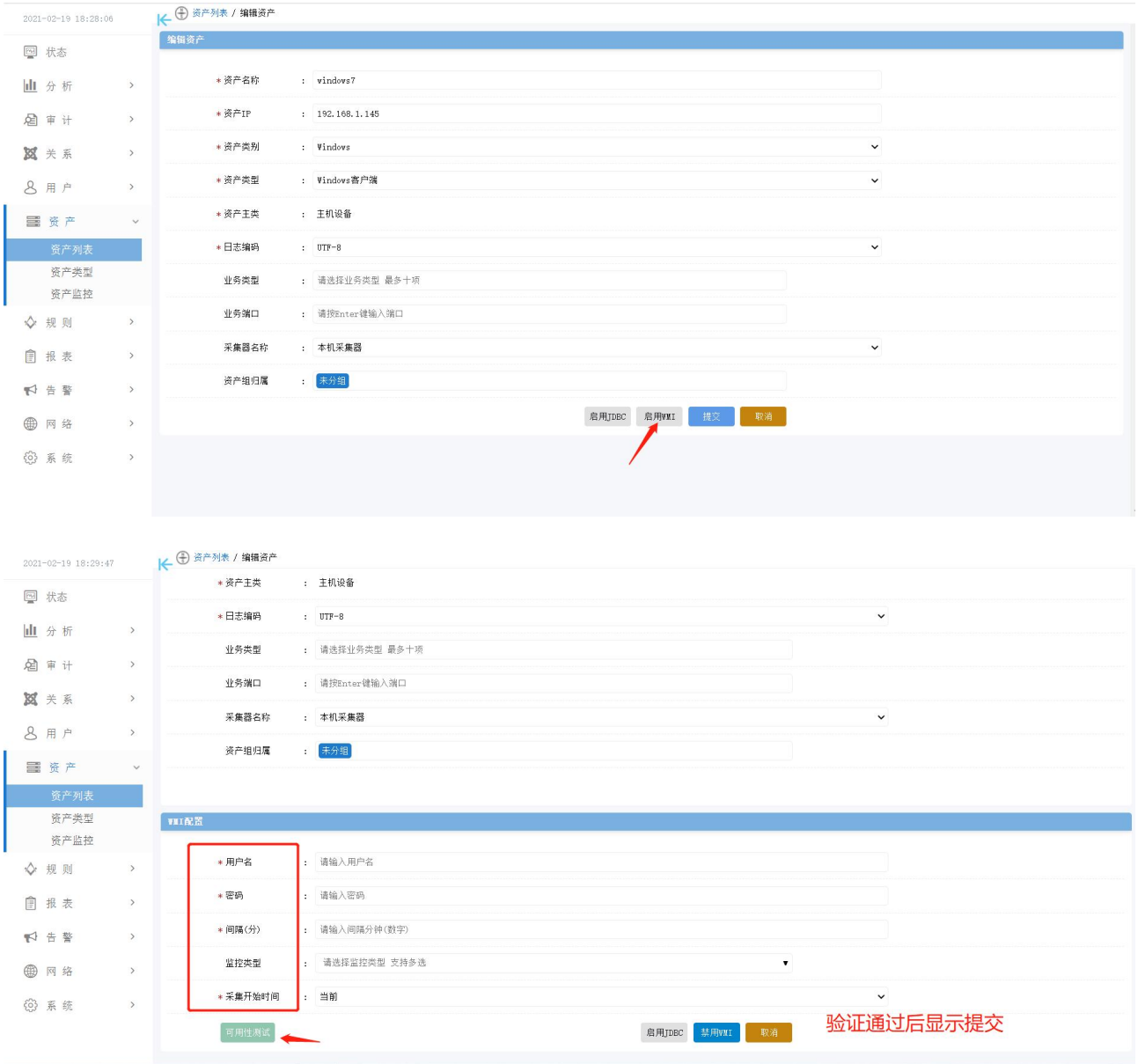
点击系统右上角‘导出资产’按钮，即可下载包含所有资产的 xlsx 文件。

7.1.8 钻取资产事件

点击每条资产信息‘操作’列中的‘查看事件’图标，可查看该资产对应的所有事件。

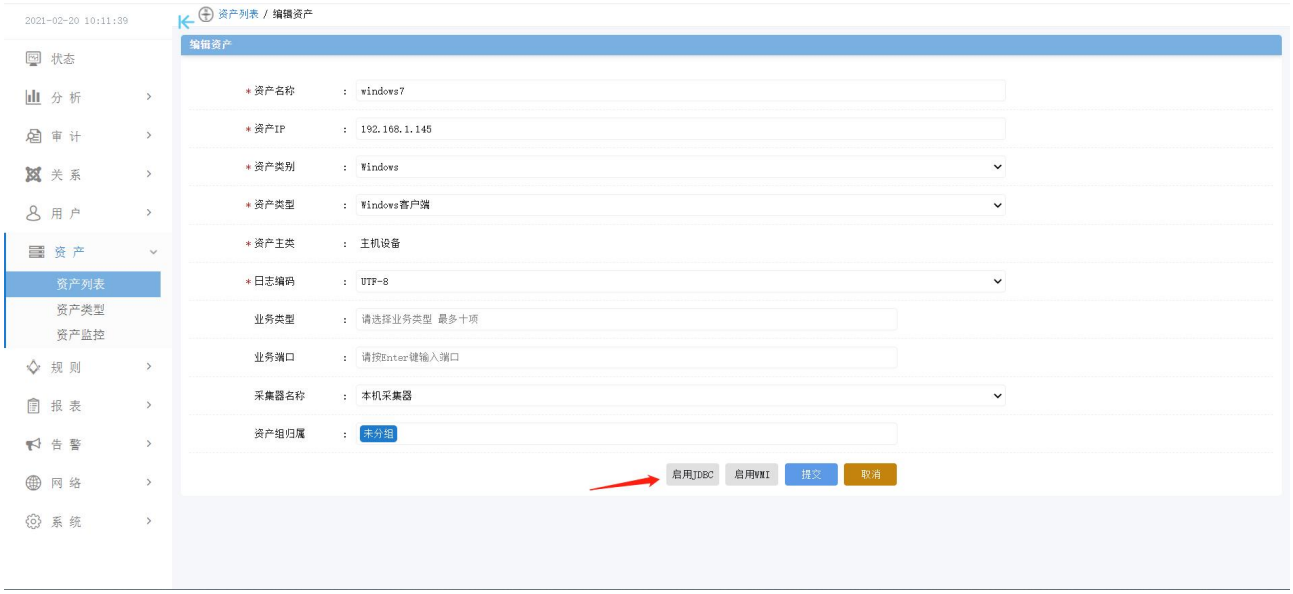
7.1.9 配置 WMI

进入编辑/添加资产界面，填写‘资产名称’‘资产 IP’项，点击‘配置选项’按钮，选择‘启动 WMI’项，显示 WMI 配置界面，填写配置项内容，点击‘测试连接’按钮，测试通过之后显示‘提交’按钮。点击‘提交’完成配置 WMI 操作。（注：Windows 必须开启 WMI 功能）

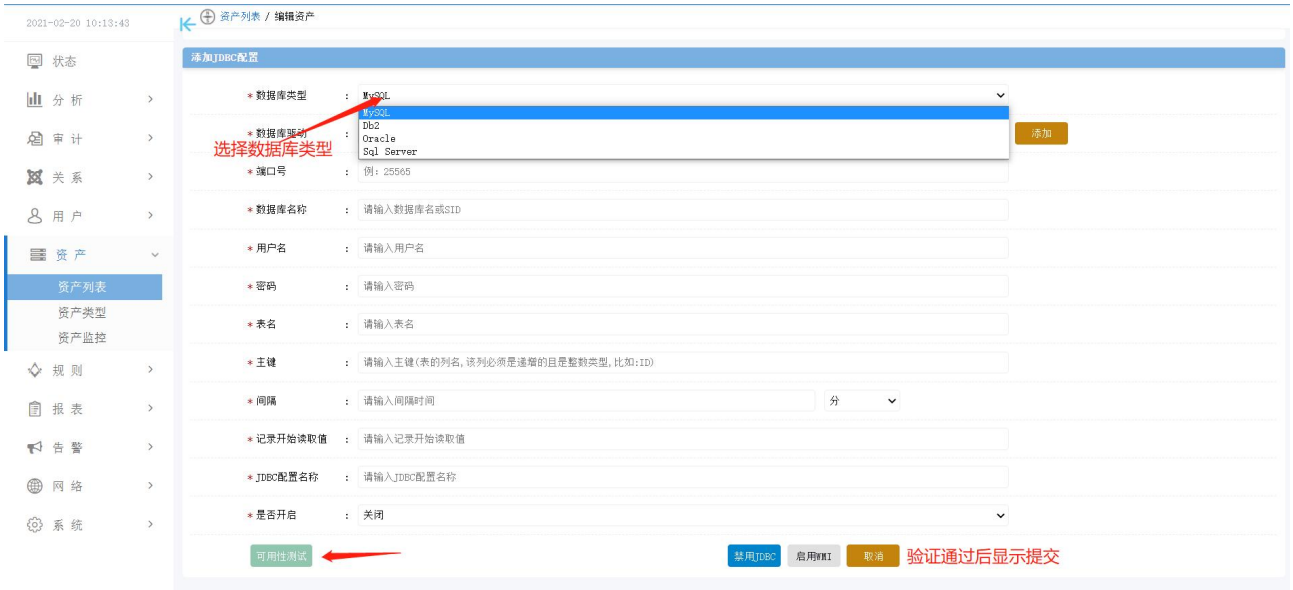


7.1.10 配置 JDBC

进入编辑/添加资产界面，填写‘资产名称’‘资产 IP’项，点击‘配置选项’按钮，选择‘启动 JDBC’项，显示 JDBC 配置界面，填写配置项内容，点击‘可用性测试’按钮，测试通过之后显示‘提交’按钮。点击‘提交’完成配置 JDBC 操作。


2021-02-20 10:11:39
资产列表 / 编辑资产
编辑资产
状态
分 析
审 计
关 系
用 户
资 产
资产列表
资产类型
资产监控
规 则
报 表
告 警
网 络
系 统
* 资产名称 : windows7
* 资产IP : 192.168.1.145
* 资产类别 : Windows
* 资产类型 : Windows客户端
* 资产主类 : 主机设备
* 日志编码 : UTF-8
业务类型 : 请选择业务类型 最多十项
业务端口 : 请按Enter键输入端口
采集器名称 : 本机采集器
资产组归属 : 未分组
启用JDBC
启用WMI
提交
取消

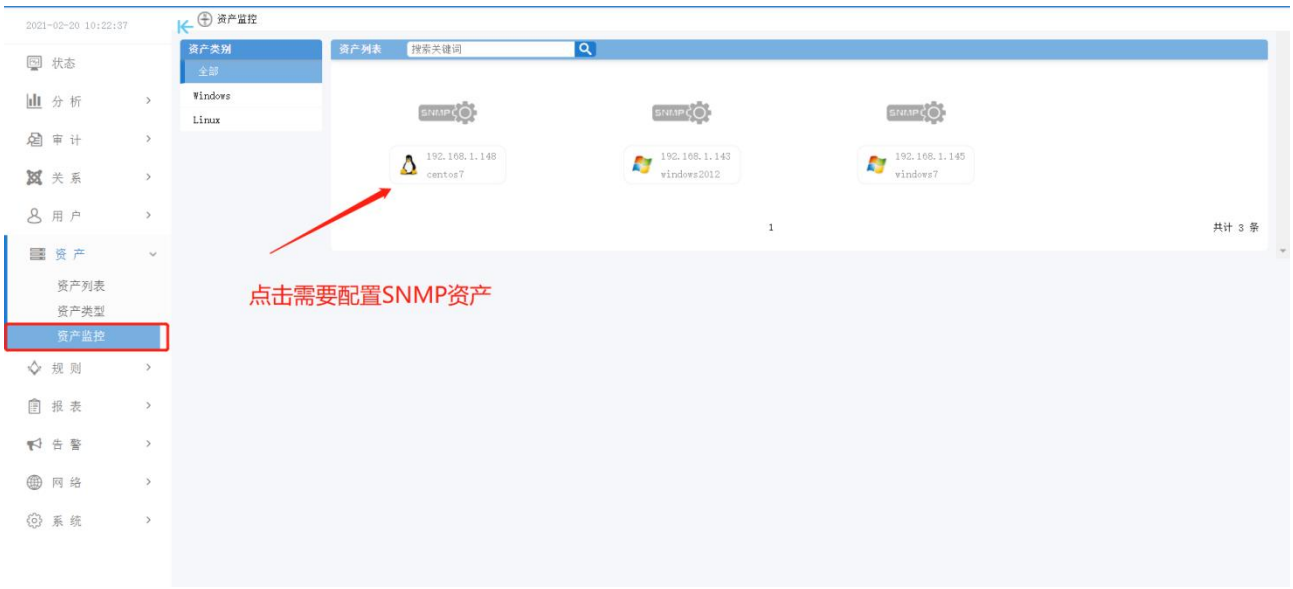

2021-02-20 10:12:29
资产列表 / 编辑资产
编辑资产
状态
分 析
审 计
关 系
用 户
资 产
资产列表
资产类型
资产监控
规 则
报 表
告 警
网 络
系 统
* 资产名称 : windows7
* 资产IP : 192.168.1.145
* 资产类别 : Windows
* 资产类型 : Windows客户端
* 资产主类 : 主机设备
* 日志编码 : UTF-8
业务类型 : 请选择业务类型 最多十项
业务端口 : 请按Enter键输入端口
采集器名称 : 本机采集器
资产组归属 : 未分组
禁用JDBC
启用WMI
提交
取消
点击添加JDBC
JDBC配置列表
数据库类型
IP地址
主键
状态
JDBC配置名称
操作

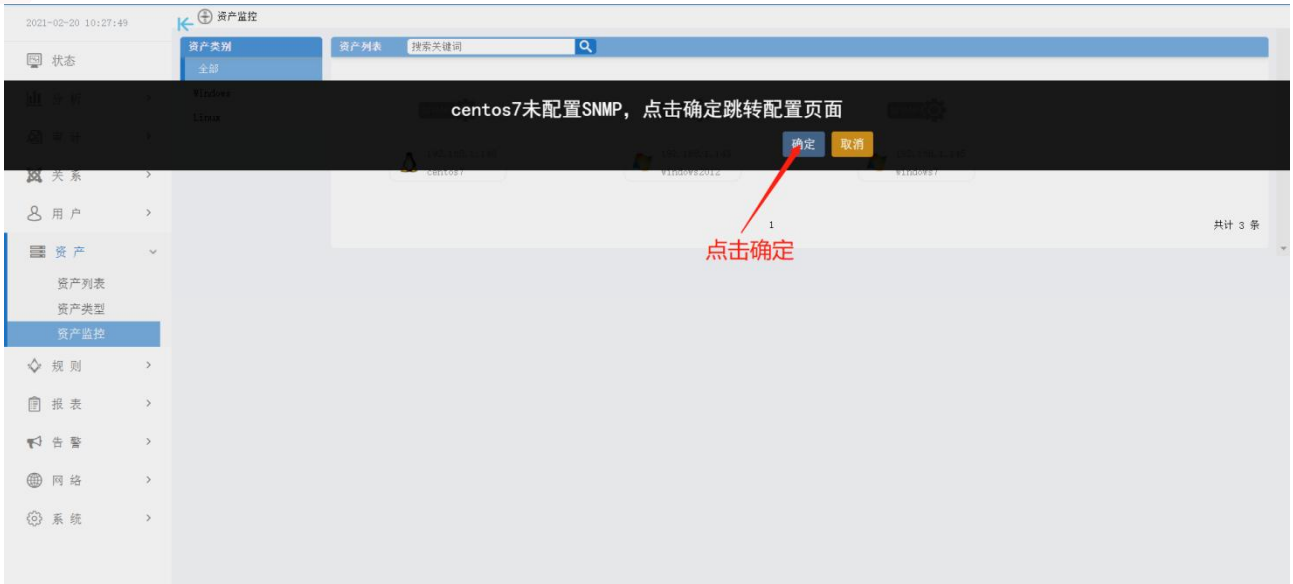


7.1.11 配置 SNMP

获取 CPU/内存/网络流量信息

进入资产→资产监控界面，选择相应资产，显示 SNMP 配置界面，填写配置项内容，点击‘测试连接’按钮，测试通过之后显示‘提交’按钮。点击‘提交’完成配置 SNMP 操作。



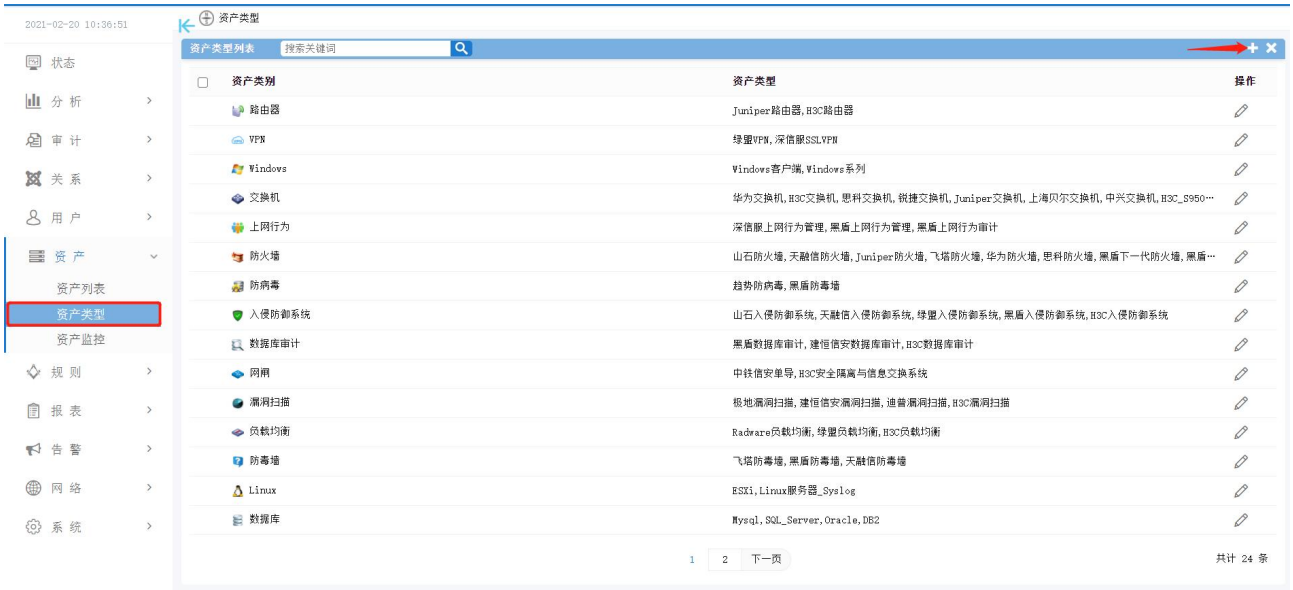


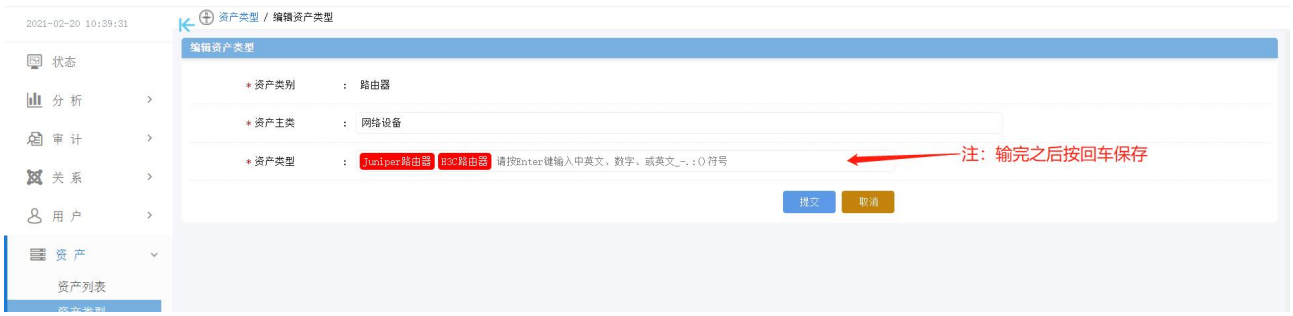
7.2 资产类型

菜单项‘资产’→‘资产类型’子项。

7.2.1 添加资产类型

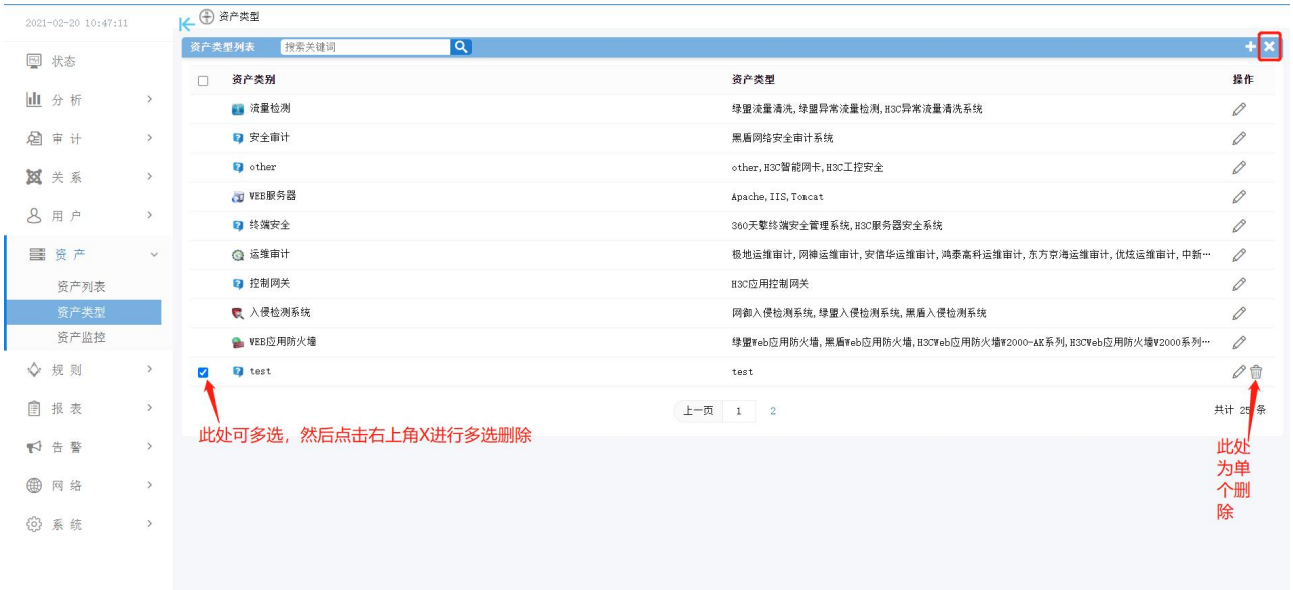
点击资产类型列表右上角‘添加’图标，进入添加资产类型界面，资产类别和资产类型（资产类型支持多个填写）→点击‘提交’完成添加资产类型的操作。





7.2.2 删除资产类型

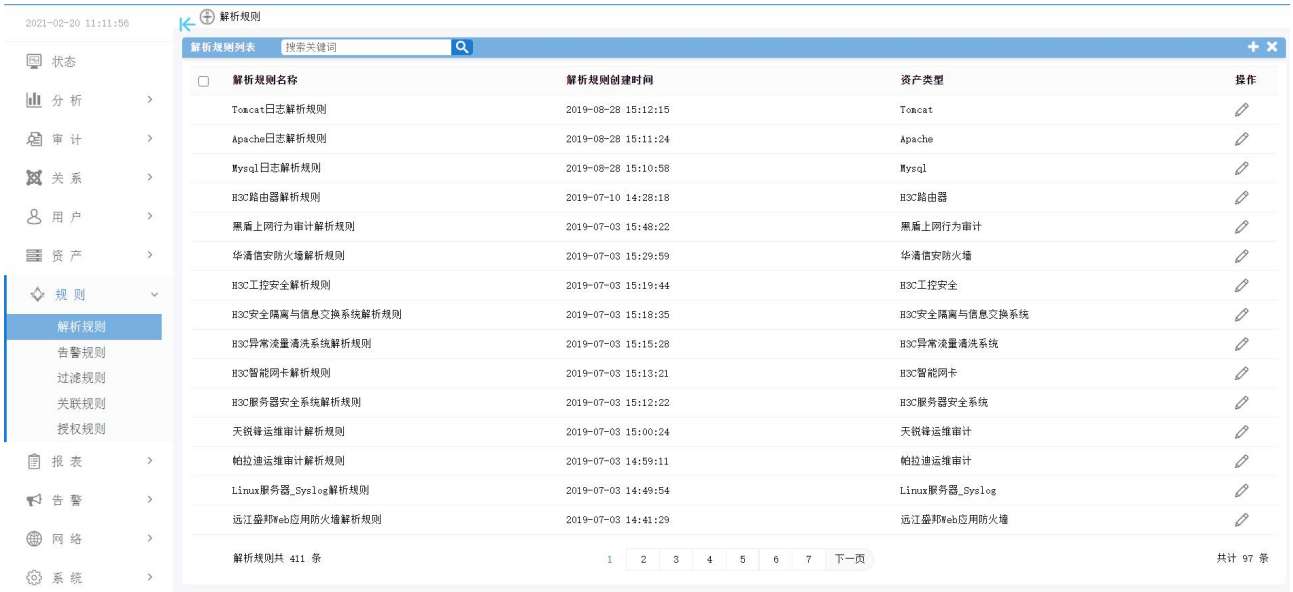
点击资产类型列表标题行左侧的复选框，可选中该页所有资产类型，点击每条资产类型左侧的复选框则可选中该条资产→点击资产列表右上角删除按钮，系统提示：确定要删除吗？点击确定，完成批量删除资产类型的操作。点击每条资产类型‘操作’列‘删除’图标，系统提示：确定要删除吗？点击确定，完成删除资产类型的操作。系统内置的资产类型不支持删除。


2021-02-20 10:47:11
状态
分 析
审 计
关 系
用 户
资 产
资产列表
资产类型
资产监控
规 则
报 表
告 警
网 络
系 统
资产类型
资产类型列表
搜索关键词
资产类别
资产类型
操作
流量检测
绿盟流量清洗, 绿盟异常流量检测, H3C异常流量清洗系统
安全审计
黑盾网络安全审计系统
other
other, H3C智能网卡, H3C工控安全
WEB服务器
Apache, IIS, Tomcat
终端安全
360天擎终端安全管理系统, H3C服务器安全系统
运维审计
极地运维审计, 网神运维审计, 安信华运维审计, 鸿泰高科运维审计, 东方京海运维审计, 优炫运维审计, 中新…
控制网关
H3C应用控制网关
入侵检测系统
网御入侵检测系统, 绿盟入侵检测系统, 黑盾入侵检测系统
WEB应用防火墙
绿盟Web应用防火墙, 黑盾Web应用防火墙, H3C Web应用防火墙W2000-AX系列, H3C Web应用防火墙W2000系列…
test
test
上一页
1
2
共计 25 条
此处可多选，然后点击右上角X进行多选删除
此处为单个删除

八. 规则

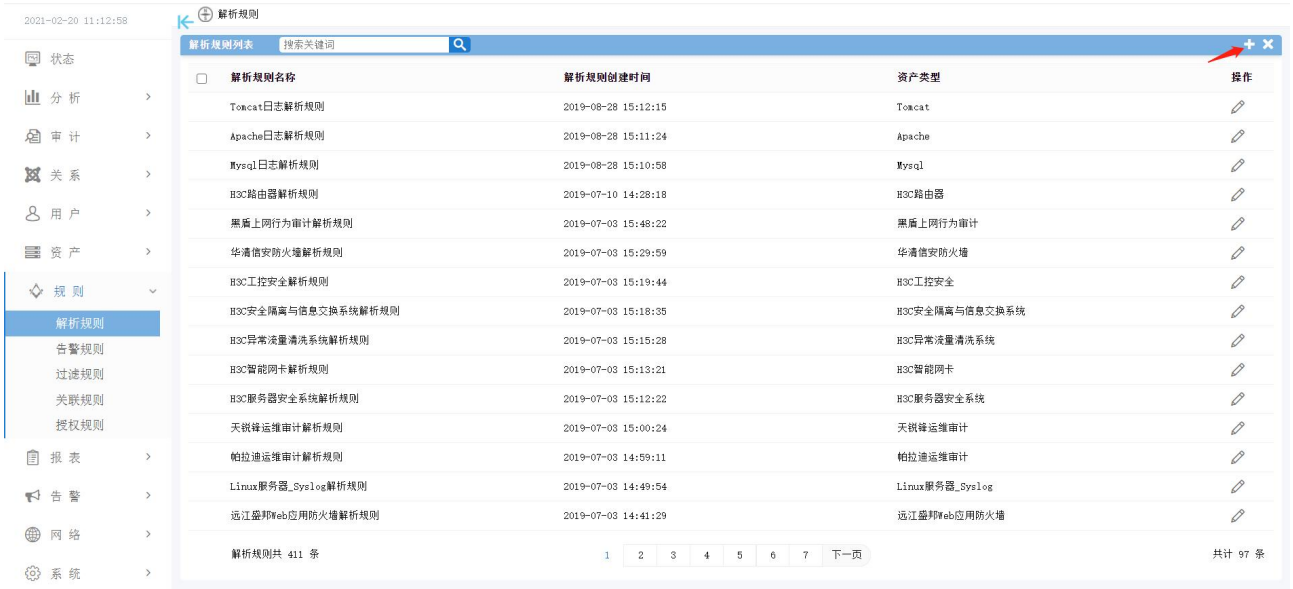
8.1 解析规则

菜单项‘规则’→‘解析规则’子项。进入解析规则列表展示页面。



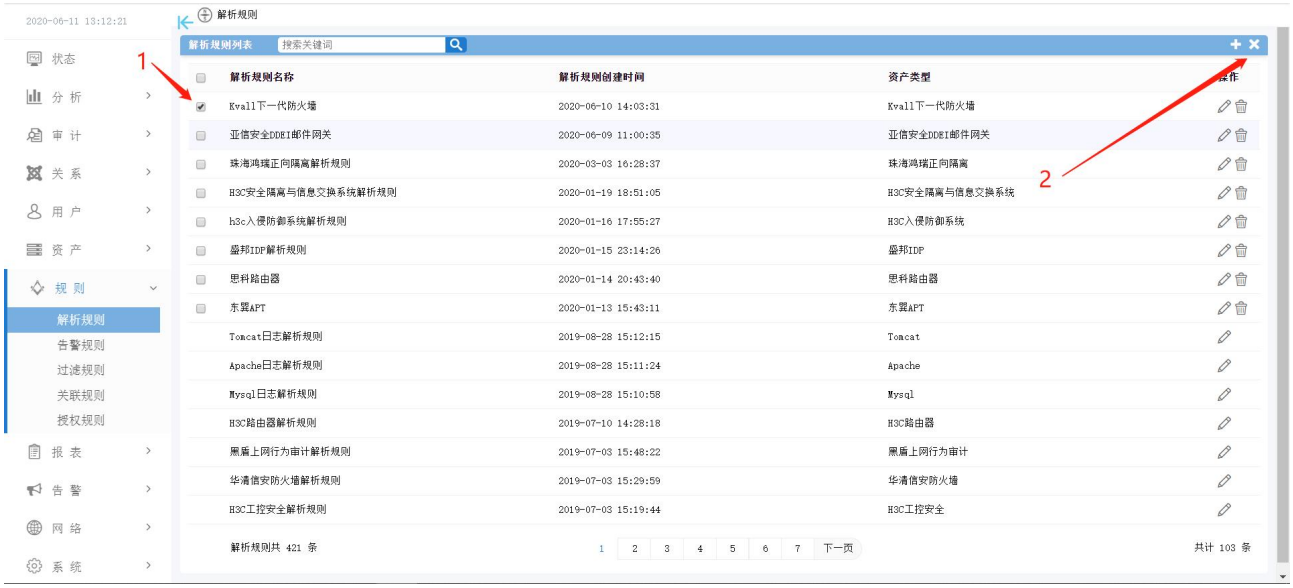
8.1.1 添加解析规则

点击解析规则列表右上角‘添加解析规则’图标，进入添加解析规则界面，填写相应的添加项，上传解析规则文件→点击‘可用性测试’，测试通过则显示‘提交’按钮，可点击‘提交’完成添加解析规则的操作。



8.1.2 删除解析规则

点击解析规则列表标题行左侧的复选框，可选中该页所有解析规则，点击每条解析规则左侧的复选框则可选中该条解析规则→点击解析规则列表右上角‘删除’按钮，系统提示：确定删除所选项吗？点击‘确定’，完成批量删除解析规则的操作。点击每条解析规则‘操作’列‘删除’图标，系统提示：确定删除此项吗？点击‘确定’，完成删除解析规则的操作。



8.2 告警规则

菜单项‘规则’→‘告警规则’子项。进入告警规则列表展示页面。

8.2.1 添加告警规则

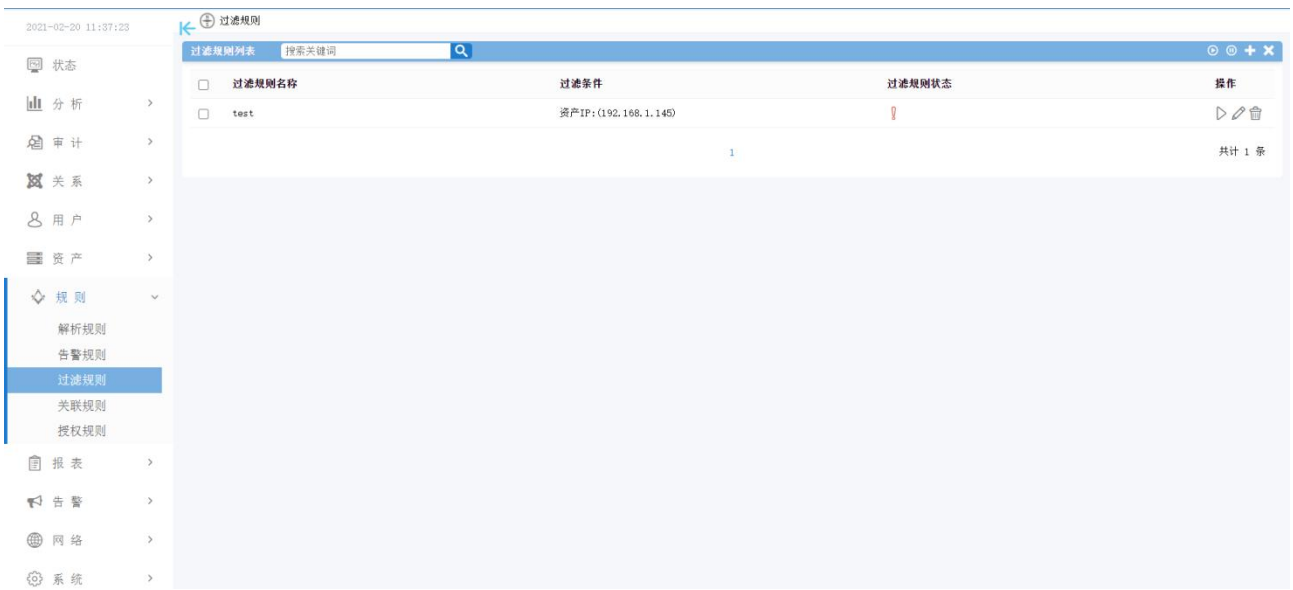
点击告警规则列表右上角‘添加’图标，进入添加告警规则界面，按要求填写相应的添加项→点击‘提交’完成添加告警规则的操作。

8.2.2 删除告警规则

点击告警规则列表标题行左侧的复选框，可选中该页所有告警规则，点击每条告警规则左侧的复选框则可选中该条告警规则→点击告警规则列表右上角‘删除’按钮，系统提示：确定删除所选项吗？点击‘确定’，完成批量删除告警规则的操作。点击每条告警规则‘操作’列‘删除’图标，系统提示：确定删除此项吗？点击‘确定’，完成删除告警规则的操作。

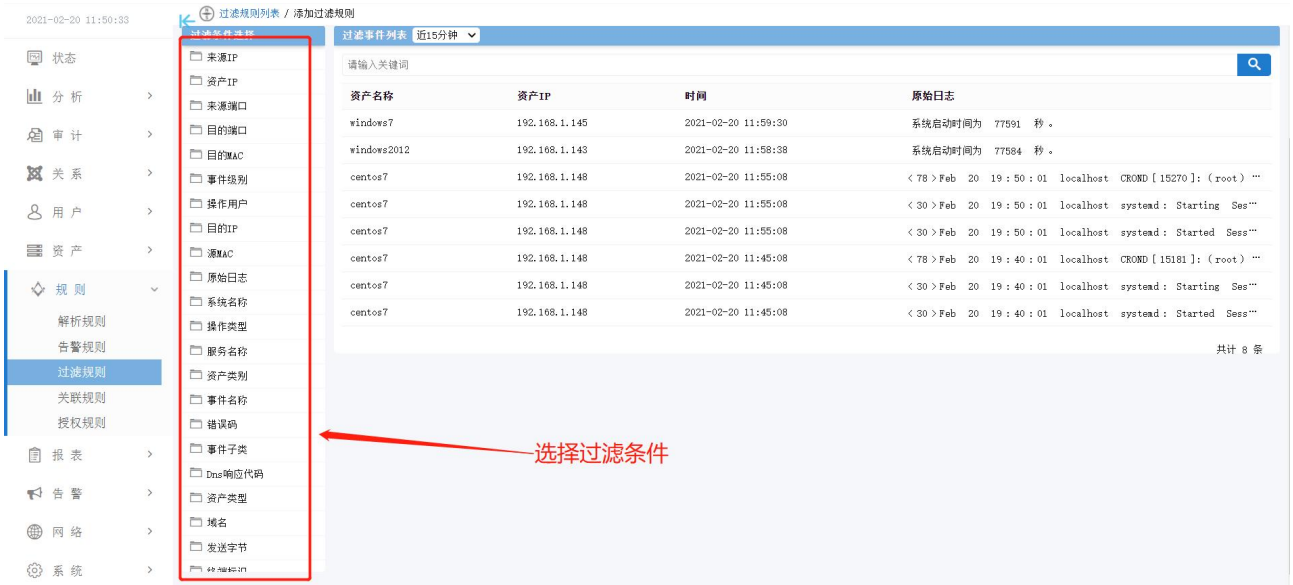
8.3 过滤规则

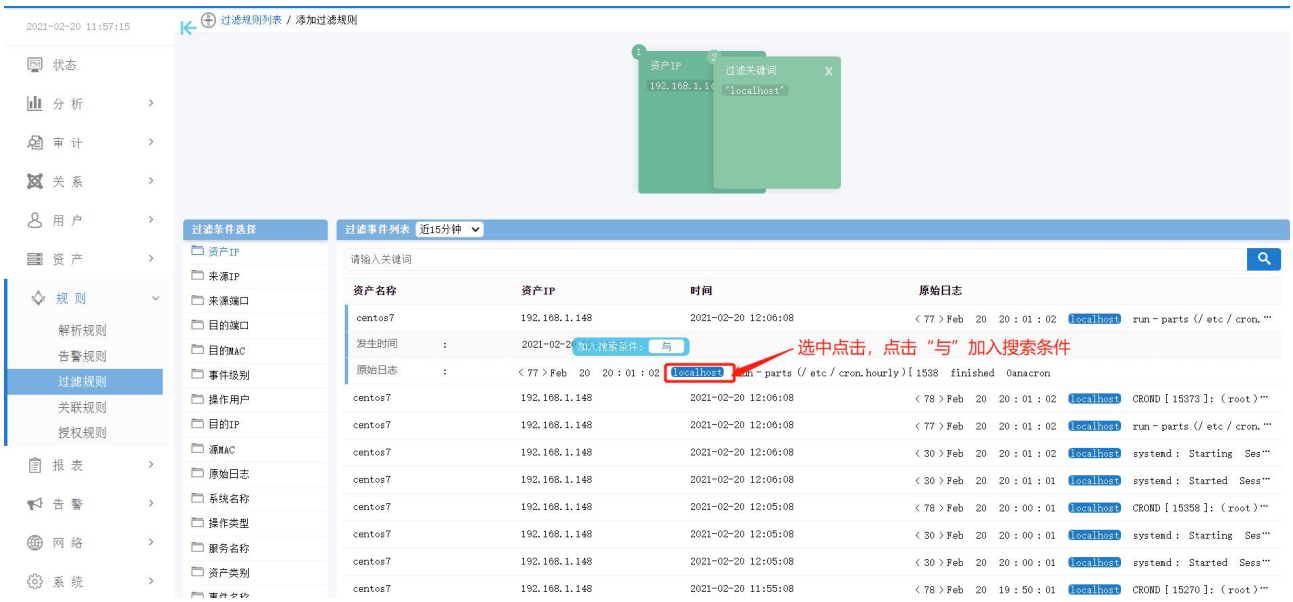
菜单项‘规则’→‘过滤规则’子项。进入过滤规则列表展示页面。



8.3.1 添加过滤规则

点击过滤规则列表右上角‘添加过滤规则’图标，进入添加过滤规则界面，可根据‘过滤条件’和‘关键字’完成过滤条件的选择，填写‘过滤规则名’，选择‘过滤规则状态’→点击‘提交’完成添加过滤规则的操作。





总机电话-- 0755-83658009 技术支持-- 0755-83658229 24 小时技术值班热线-----135-1069-3536
http://www.anysec.com 深圳市龙华区观澜街道观光路 1301-80 号电子科技大学(深圳)高等研究院 3 号楼 1401

8.3.2 删除过滤规则

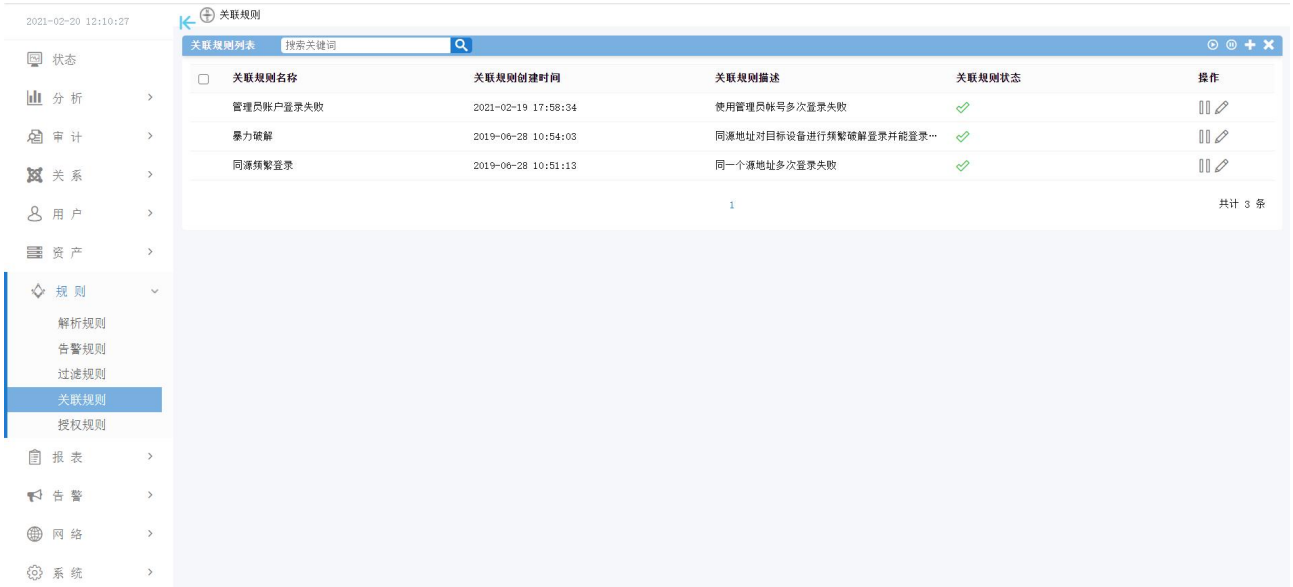
点击过滤规则列表标题行左侧的复选框，可选中该页所有过滤规则，点击每条过滤规则左侧的复选框则可选中该条过滤规则→点击过滤规则列表右上角‘删除’按钮，系统提示：确定删除所选项吗？点击‘确定’，完成批量删除过滤规则的操作。点击每条过滤规则‘操作’列‘删除’图标，系统提示：确定删除此项吗？点击‘确定’，完成删除过滤规则的操作。

8.3.3 启动过滤规则

点击过滤规则列表标题行左侧的复选框，可选中该页所有过滤规则，点击每条过滤规则左侧的复选框则可选中该条过滤规则→点击过滤规则列表右上角‘多选停止/多选开启’按钮，系统提示：确定停止/开启所选项吗？点击‘确定’，完成批量停止/开启过滤规则的操作。点击每条过滤规则‘操作’列‘开启/停止’图标，系统提示：确定停止/开启此项吗？点击‘确定’，完成停止/开启过滤规则的操作。

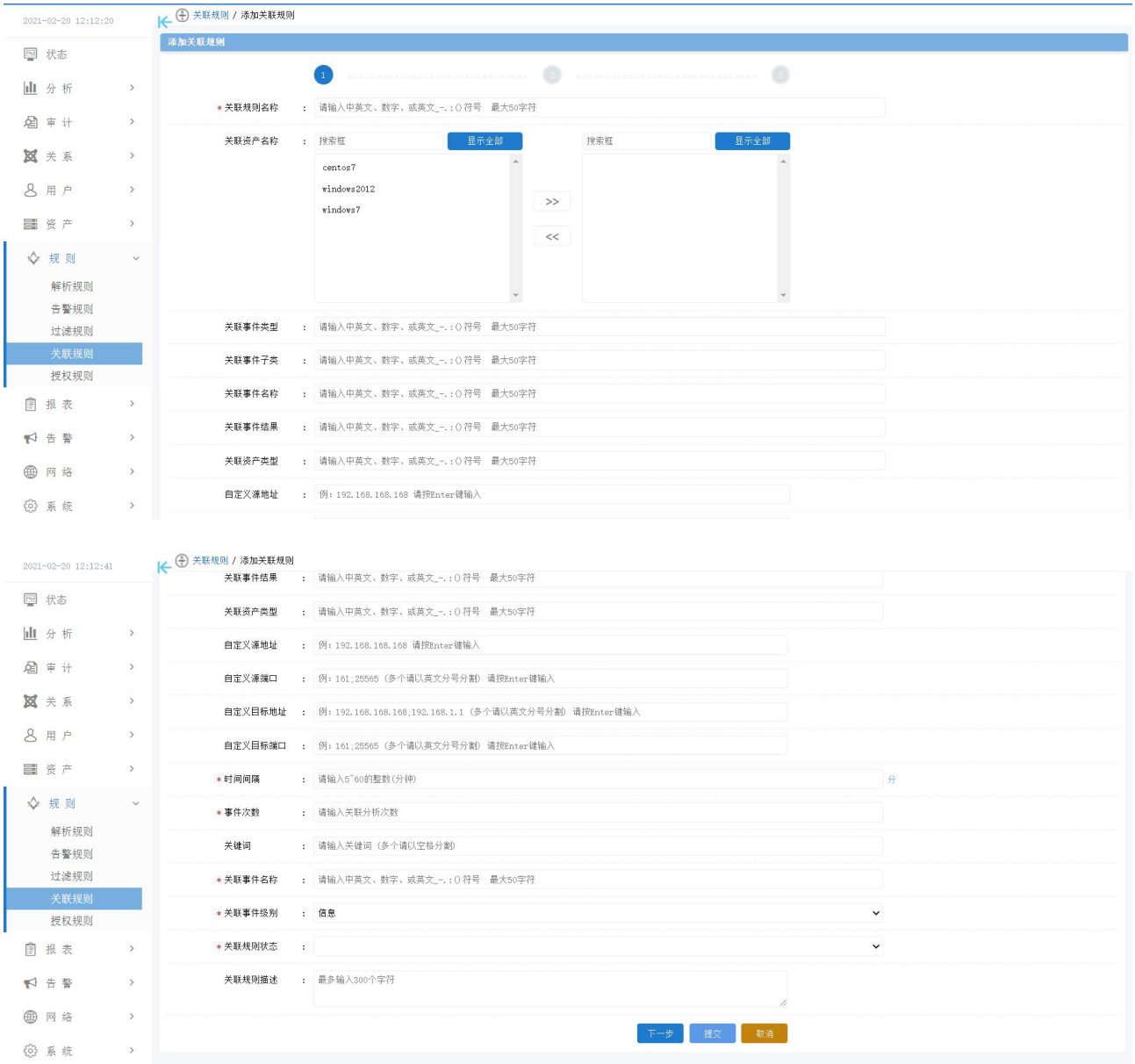
8.4 关联规则

菜单项‘规则’→‘关联规则’子项。进入关联规则列表展示页面。



8.4.1 添加关联规则

点击关联规则列表右上角‘添加关联规则’图标，进入添加关联规则界面，按要求填写相应的添加项→点击‘下一步’进入下一环节添加，或者点击‘提交’完成添加关联规则操作。



8.4.2 删除关联规则

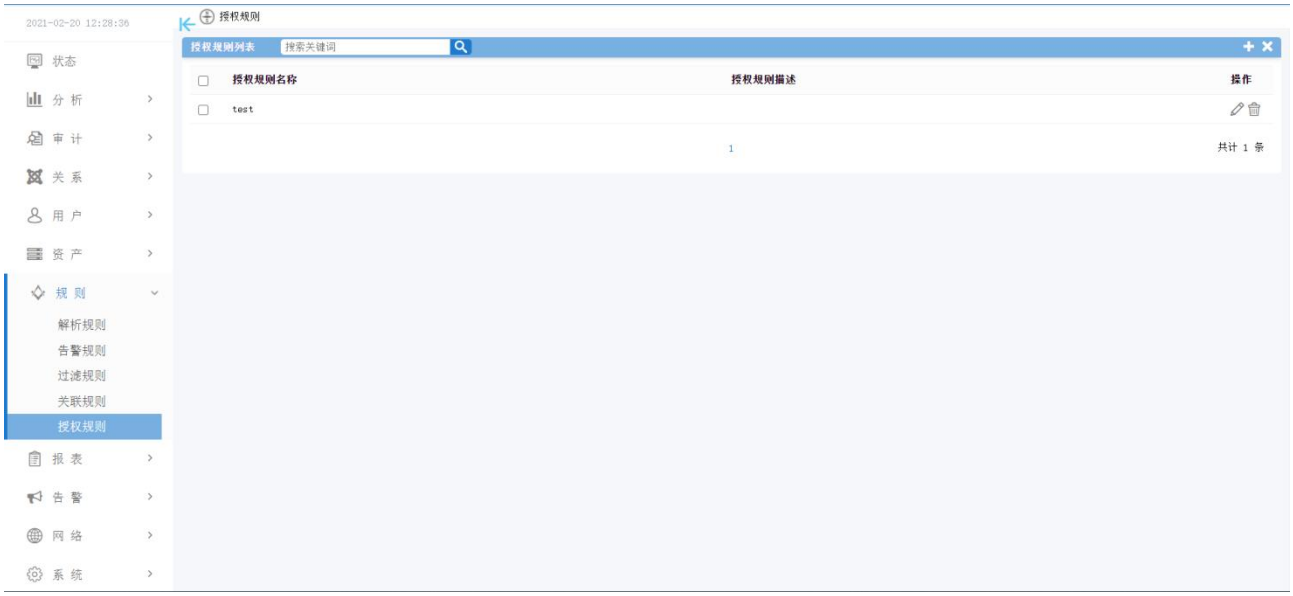
点击关联规则列表标题行左侧的复选框，可选中该页所有关联规则，点击每条关联规则左侧的复选框则可选中该条关联规则→点击关联规则列表右上角‘删除’按钮，系统提示：确定删除所选项吗？点击‘确定’，完成批量删除关联规则的操作。点击每条关联规则‘操作’列‘删除’图标，系统提示：确定删除此项吗？点击‘确定’，完成删除关联规则的操作。

8.4.3 启动/暂停关联规则

点击关联规则列表标题行左侧的复选框，可选中该页所有关联规则，点击每条关联规则左侧的复选框则可选中该条关联规则→点击关联规则列表右上角‘多选停止/多选开启’按钮，系统提示：确定停止/开启所选项吗？点击‘确定’，完成批量停止/开启关联规则的操作。点击每条关联规则‘操作’列‘开启/停止’图标，系统提示：确定停止/开启此项吗？点击‘确定’，完成停止/开启关联规则的操作。

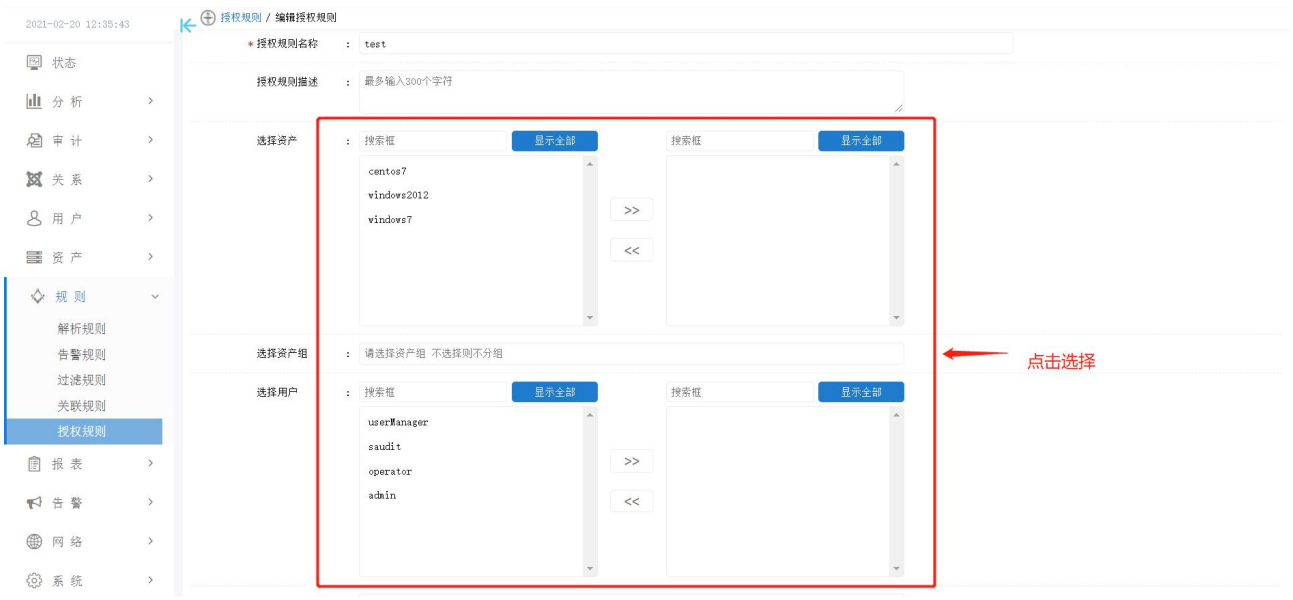
8.5 授权规则

菜单项‘规则’→‘授权规则’子项。进入授权规则列表展示页面。



8.5.1 添加授权规则

点击授权规则列表右上角‘添加’图标，进入添加授权规则界面，按要求填写和选择相应的添加项→点击‘提交’完成添加授权规则的操作。



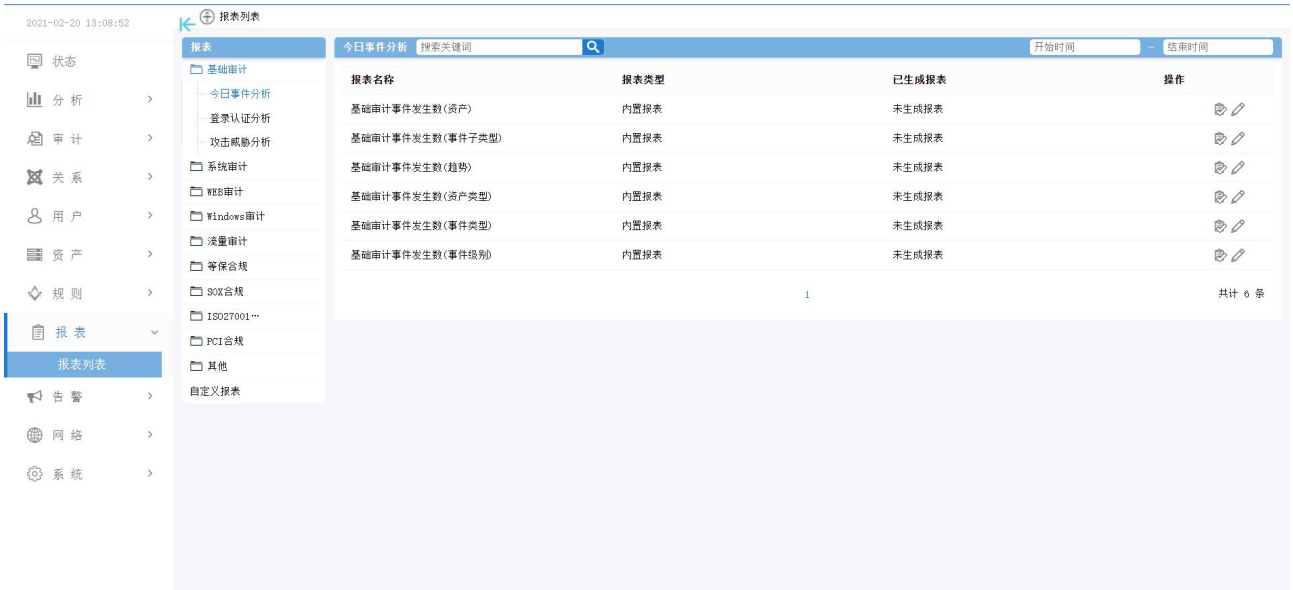
8.5.2 删除授权规则

点击授权规则列表标题行左侧的复选框，可选中该页所有授权规则，点击每条授权规则

左侧的复选框则可选中该条授权规则→点击授权规则列表右上角‘删除’按钮，系统提示：确定删除所选项吗？点击‘确定’，完成批量删除授权规则的操作。点击每条授权规则‘操作’列‘删除’图标，系统提示：确定删除此项吗？点击‘确定’，完成删除授权规则的操作。

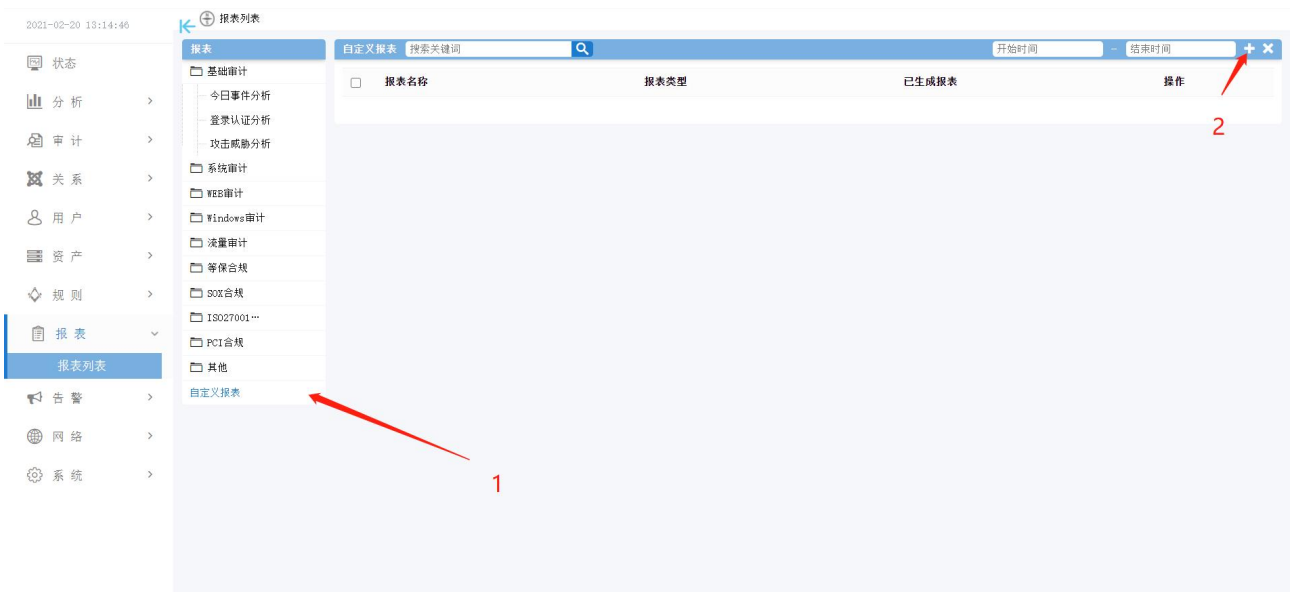
九. 报表

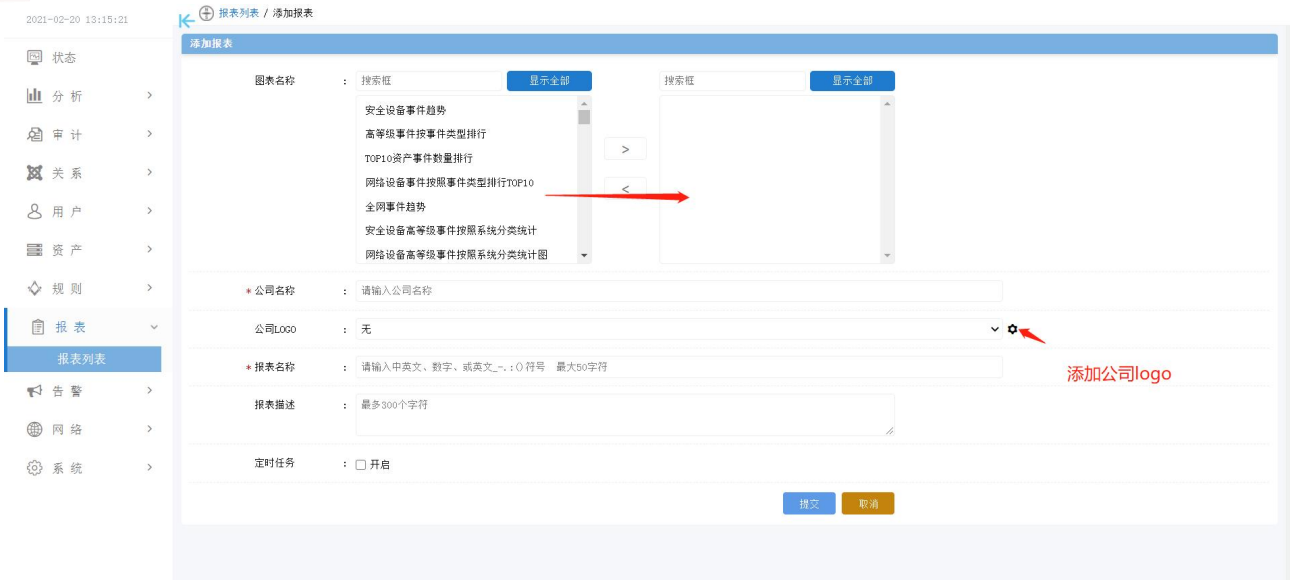
菜单项‘报表’→‘报表列表’子项。进入报表列表展示页面。



9.1 添加报表

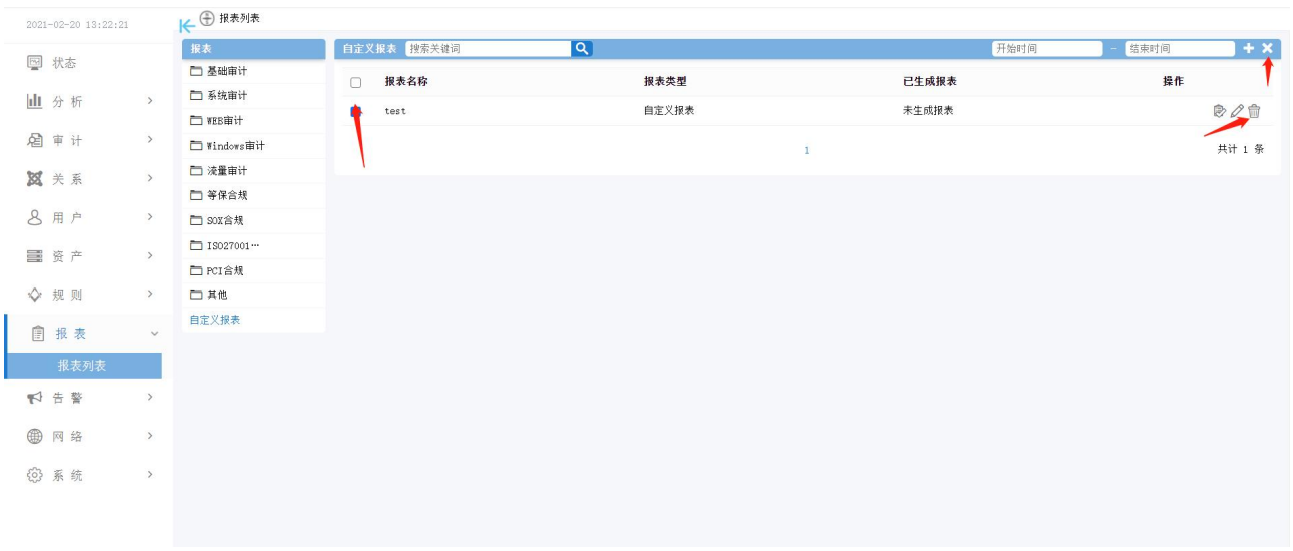
点击报表列表右上角‘添加’图标，进入添加报表界面，按要求填写，上传文件，选择需要的报表类型→点击‘提交’完成添加报表的操作。





9.2 删除报表

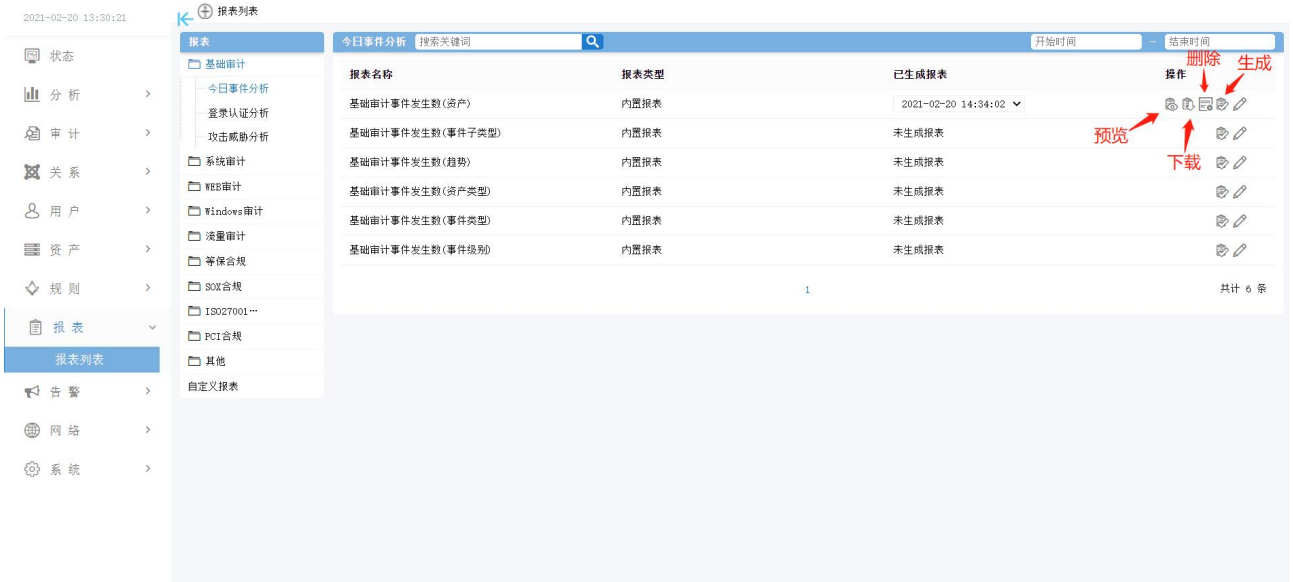
点击报表列表标题行左侧的复选框，可选中该页所有报表信息，点击每条报表信息左侧的复选框则可选中该条报表信息→点击报表列表右上角‘删除’按钮，系统提示：确定删除所选项吗？点击‘确定’，完成批量删除报表的操作。点击每条报表信息‘操作’列‘删除’图标，系统提示：确定删除此项吗？点击‘确定’，完成删除报表的操作。系统内置的报表不支持删除。



9.3 预览/下载/生成报表

点击每条报表信息‘操作’列‘生成’图标和‘报表生成时间’列的‘预览/下载’图标，

可进行报表的预览/下载/生成操作。



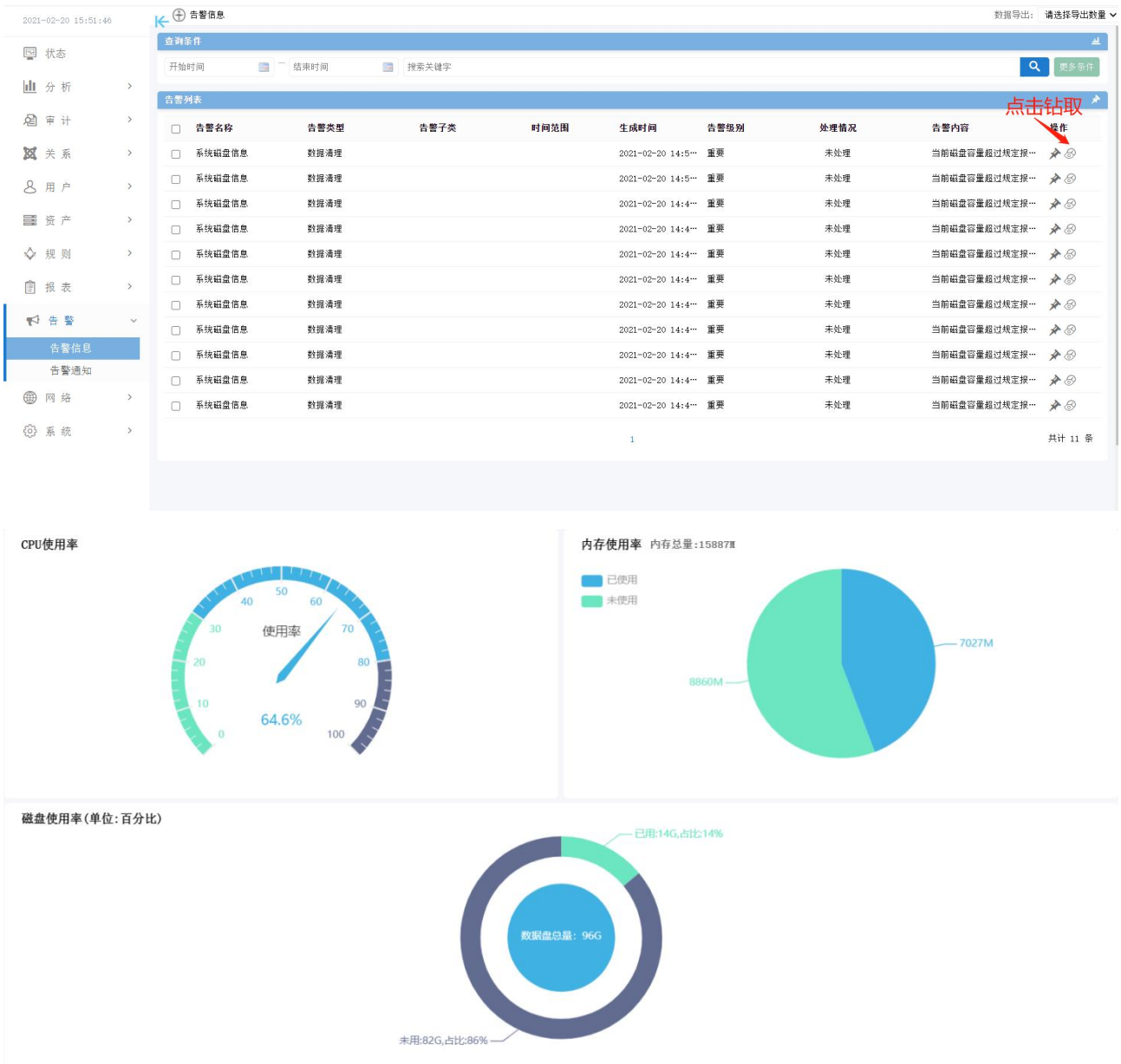
（注：先点击生成报表才会出现预览下载删除功能）

十. 告警

菜单项‘告警’→‘告警信息’子项。进入告警信息列表展示页面。

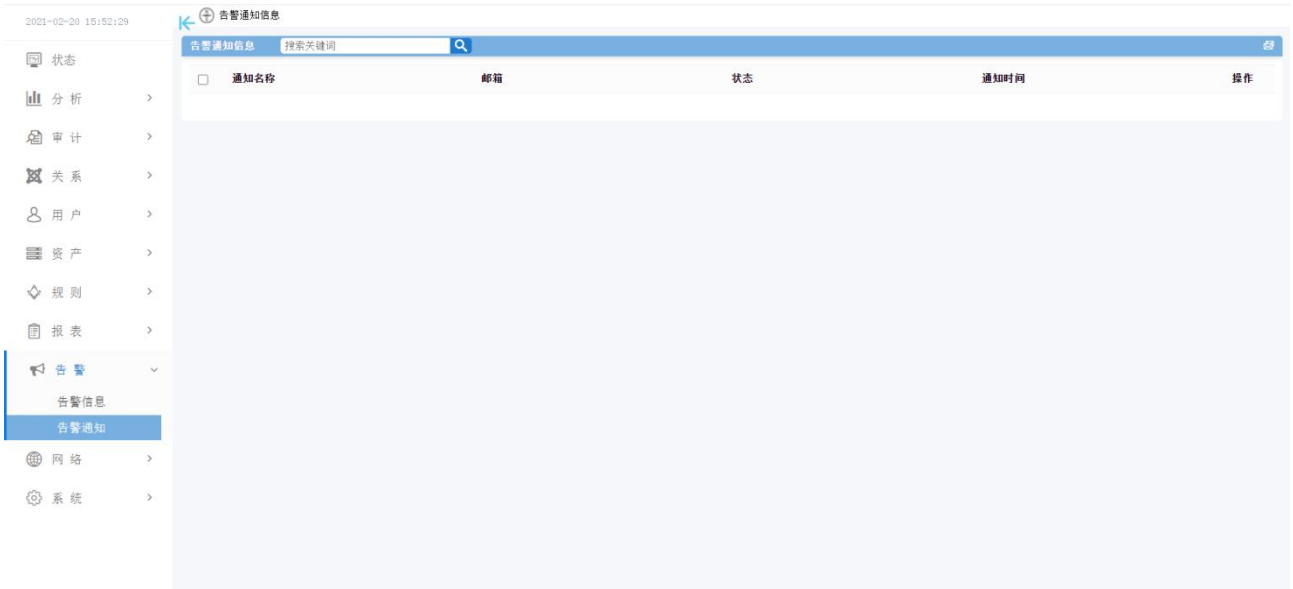
10.1 钻取告警关联事件

点击每条告警信息‘操作’列的‘查看’即可查看该条告警信息的详细情况。



10.2 告警通知

菜单项‘告警’→‘告警通知’子项。进入告警通知列表展示页面。



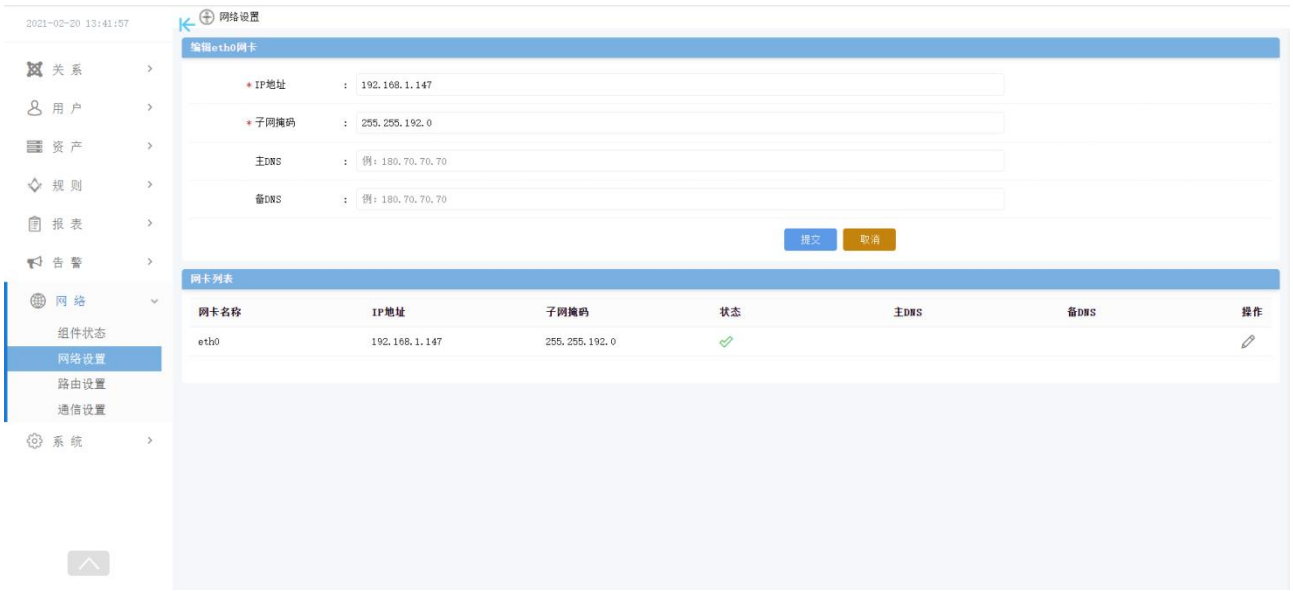
十一. 网络

11.1 组件状态

菜单项‘网络’→‘组件状态’子项。进入组件状态展示页面。可查看系统各项功能服务是否正常。

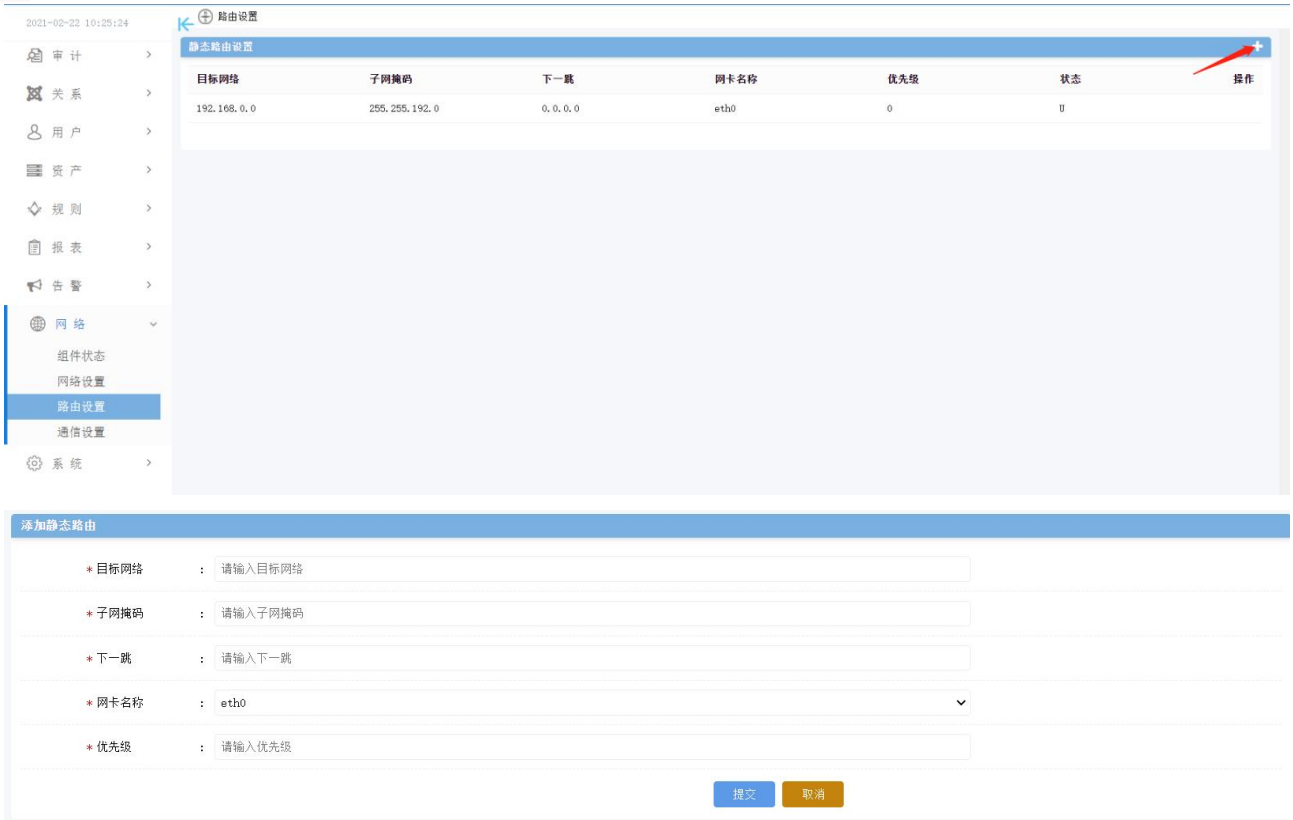
11.2 网络设置

菜单项‘网络’→‘网络设置’子项。进入网卡列表展示页面。点击操作列‘编辑’图标，可编辑对应网卡信息。



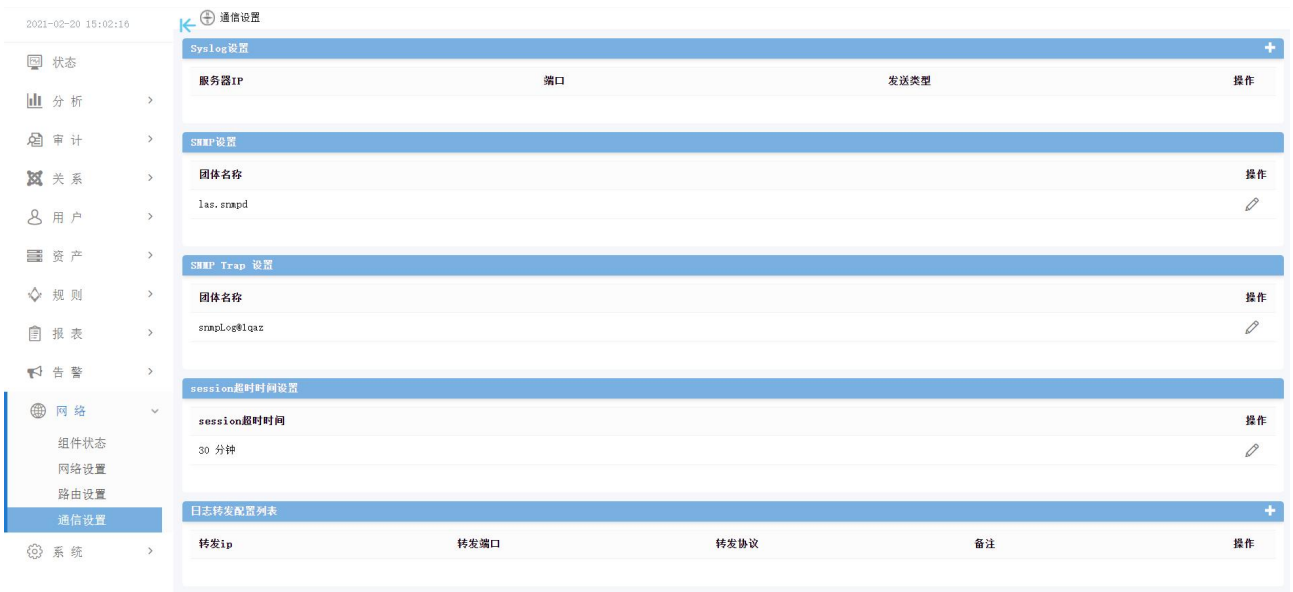
11.3 路由设置

菜单项‘网络’→‘路由设置’子项。进入路由设置展示页面。点击右上角‘添加’图标，可添加路由。



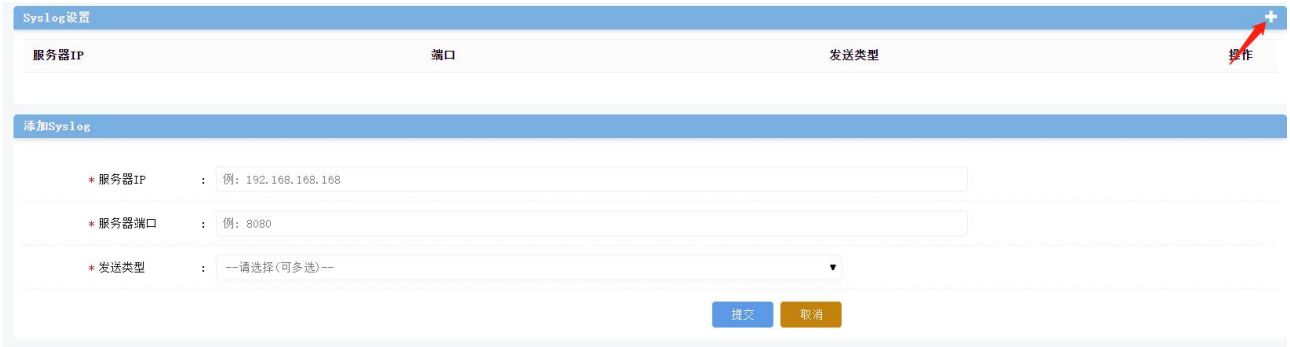
11.4 通信设置

菜单项‘网络’→‘通信设置’子项。进入 Syslog 设置列表，SNMP 设置和 session 超时时间设置页面。其中 Syslog 设置可添加删除，所有设置项均可编辑。



11.4.1 添加 syslog

点击 Syslog 设置模块的右上角的‘添加’图标，展示 Syslog 设置界面，正确填写必要信息，点击‘提交’完成添加 syslog 的操作。



11.4.2 编辑 SNMP

点击‘SNMP 设置’模块表格的操作列‘编辑’图标，显示 SNMP 设置界面，编辑完成点击‘提交’完成编辑 SNMP 操作。

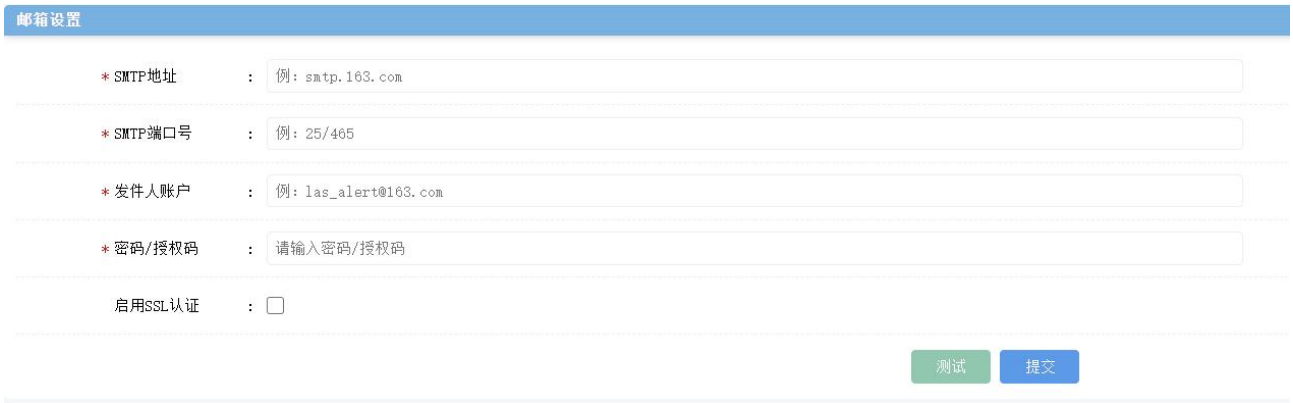
11.4.3 编辑 Session 时间

点击‘session 超时时间设置’模块表格的操作列‘编辑’图标，显示 session 超时时间设置界面，编辑完成点击‘提交’完成编辑 session 时间操作。

十二. 系统

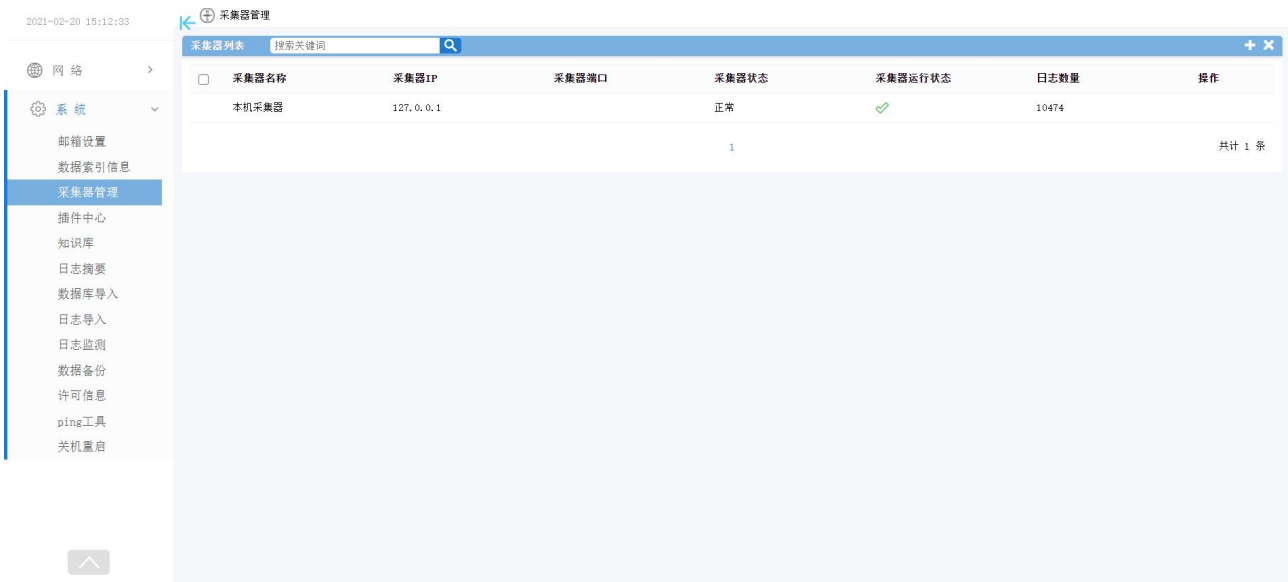
12.1 邮箱设置

菜单项‘系统’→‘邮箱设置’子项。进入告警邮箱设置页面，填写必要的提交信息，如果选择‘启用密码认证’，则‘SMTP 密码’项也作为必填项。



12.2 采集器管理

菜单项‘系统’→‘采集器管理’子项。进入采集器列表界面。



12.2.1 添加采集器

点击采集器列表右上角‘添加’图标，进入添加采集器界面，按要求填写提交项信息→点击‘可用性测试’，测试通过显示‘提交’按钮→完成添加采集器的操作。

12.3 插件中心

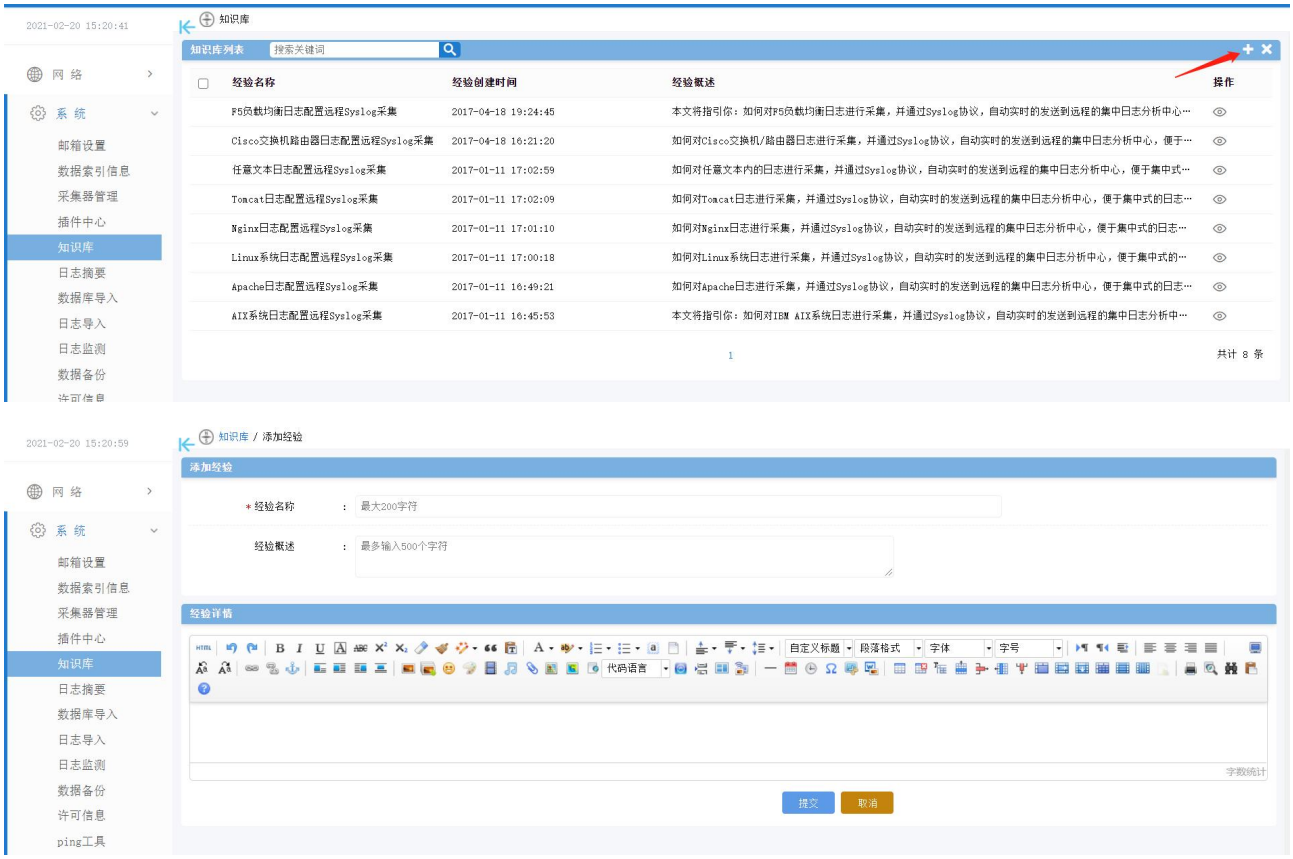
菜单项‘系统’→‘插件中心’子项。进入插件列表界面。点击每条插件信息‘操作’列‘下载’图标，可下载对应的版本的插件。

12.4 知识库

菜单项‘系统’→‘知识库’子项。进入知识库模块页面。

12.4.1 添加经验

点击知识库列表右上角‘添加’图标，进入添加经验界面，按要求填写提交项信息→点击‘提交’完成添加经验的操作。

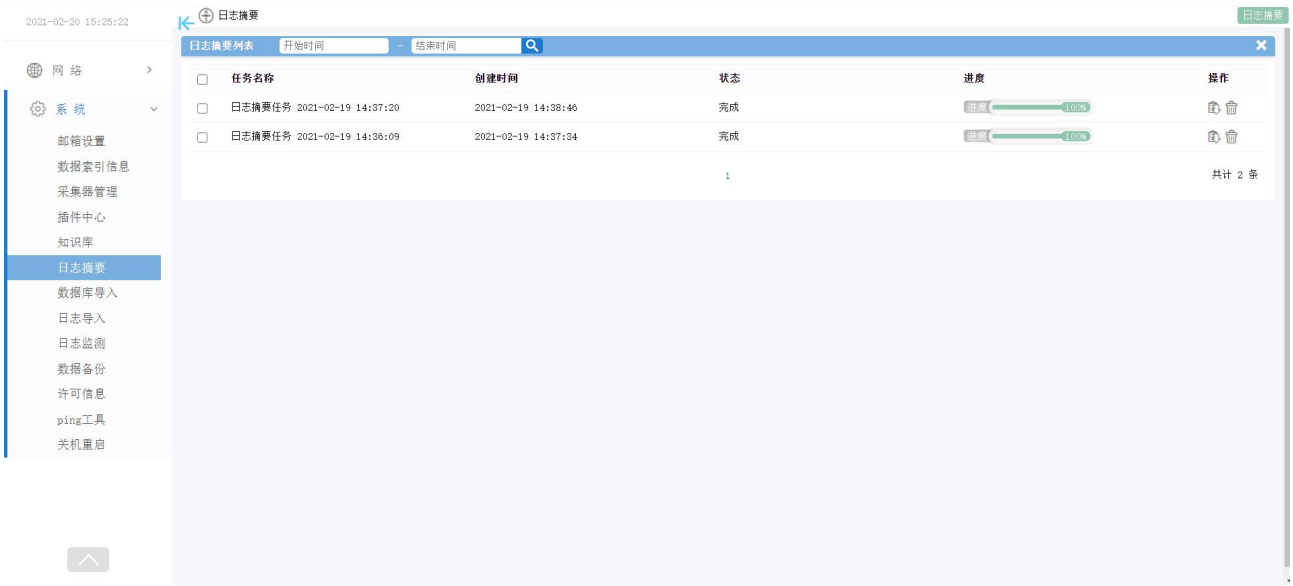


12.4.2 预览经验

点击每条知识库信息‘操作’列‘查看经验’图标，可查看该条知识库的详细信息。

12.5 日志摘要

菜单项‘系统’→‘日志摘要’子项。进入日志摘要模块页面。

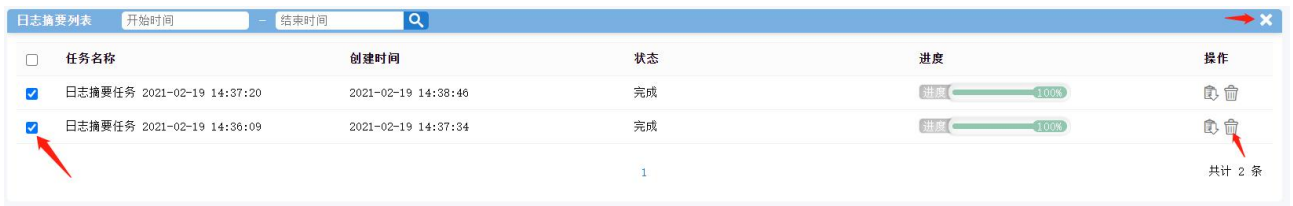


12.5.1 添加日志摘要

点击日志摘要列表右上角‘日志摘要’按钮，进入添加日志摘要界面，选择必要提交项→点击‘启动’完成添加日志摘要的操作。

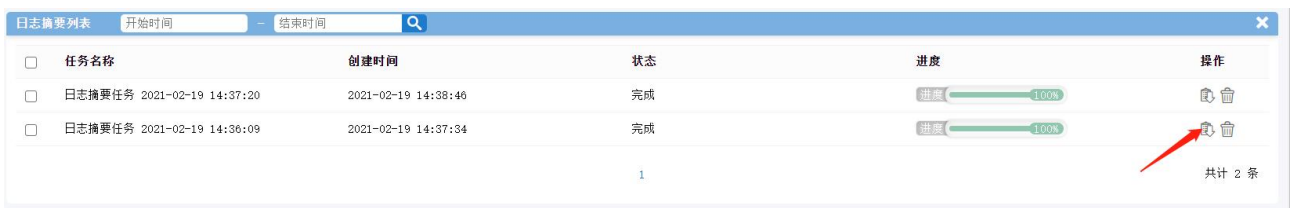
12.5.2 日志摘要删除

点击日志摘要列表标题行左侧的复选框，可选中该页所有日志摘要，点击每条日志摘要左侧的复选框则可选中该条日志摘要→点击日志摘要列表右上角‘删除’按钮，系统提示：确定删除所选项吗？点击‘确定’，完成批量删除日志摘要的操作。点击每条日志摘要信息‘操作’列‘删除’图标，系统提示：确定删除此项吗？点击‘确定’，完成删除日志摘要的操作。



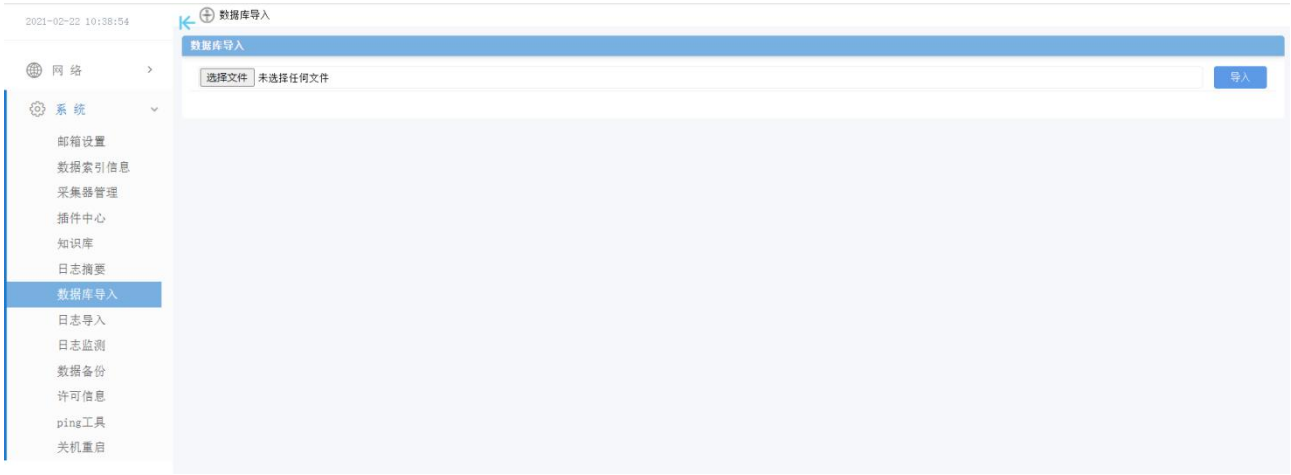
12.5.3 日志摘要下载

点击每条日志摘要信息‘操作’列‘下载’图标，系统提示：确定下载该条任务结果吗？点击‘确定’，完成下载日志摘要的操作。



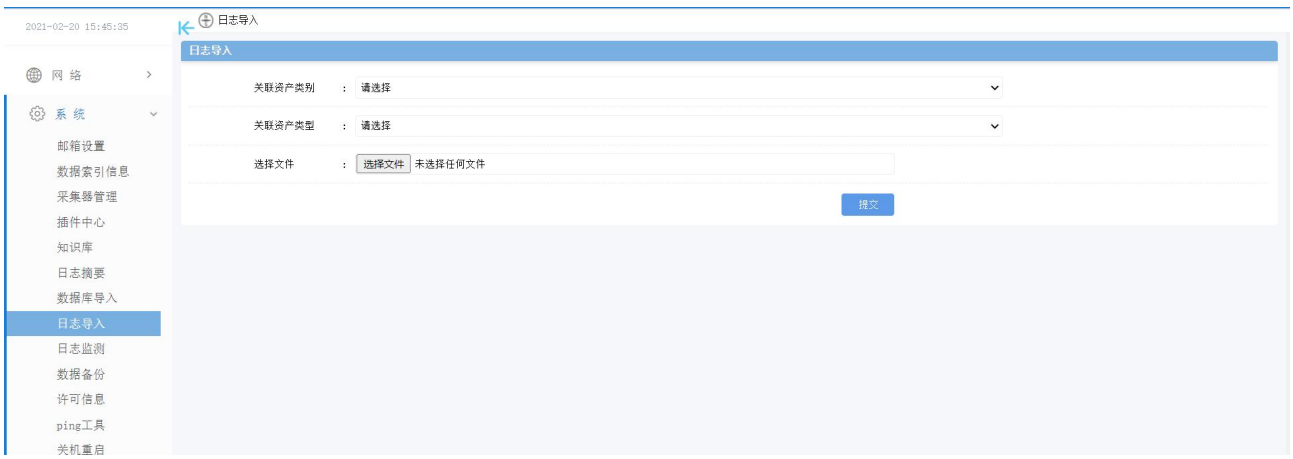
12.6 数据库导入

菜单项‘系统’→‘数据备份’子项。进入数据库导入模块。



12.7 日志导入

菜单项‘系统’→‘日志导入’子项。进入日志导入模块。选择‘关联设备类别’，上传完整日志.log 文件，点击‘提交’按钮，完成日志导入操作。

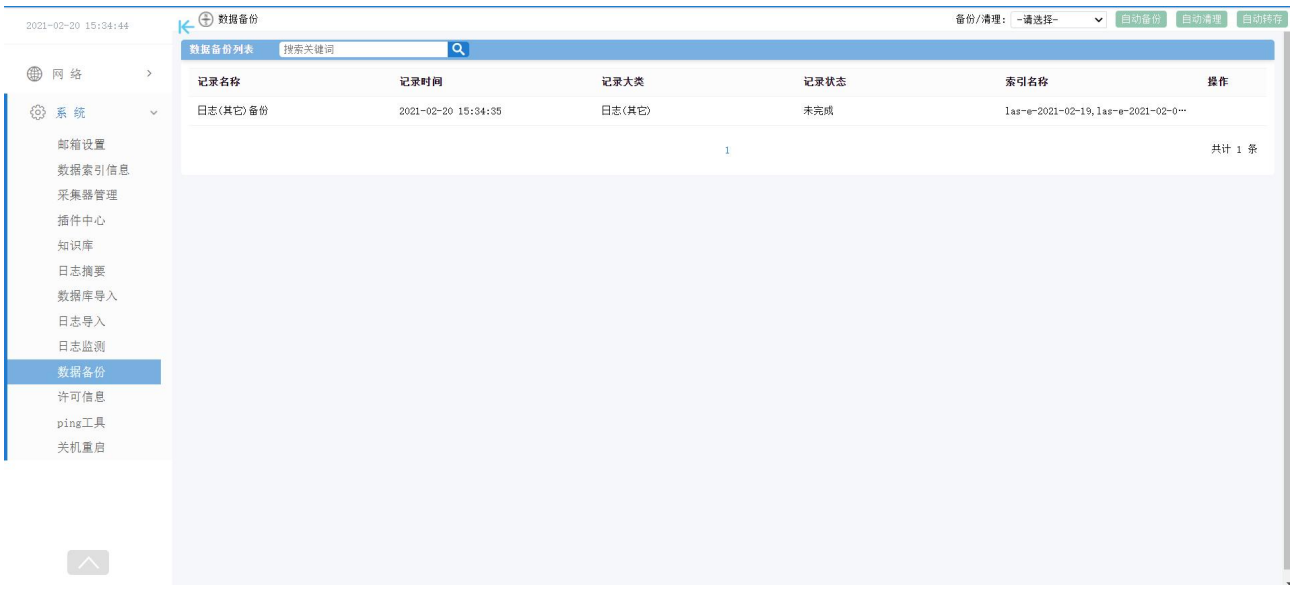


12.8 日志监测

菜单项‘系统’→‘日志监测’子项。进入日志监测模块。可以监测系统是否可以采集到客户端日志。

12.9 数据备份

菜单项‘系统’→‘数据备份’子项。进入数据备份模块。

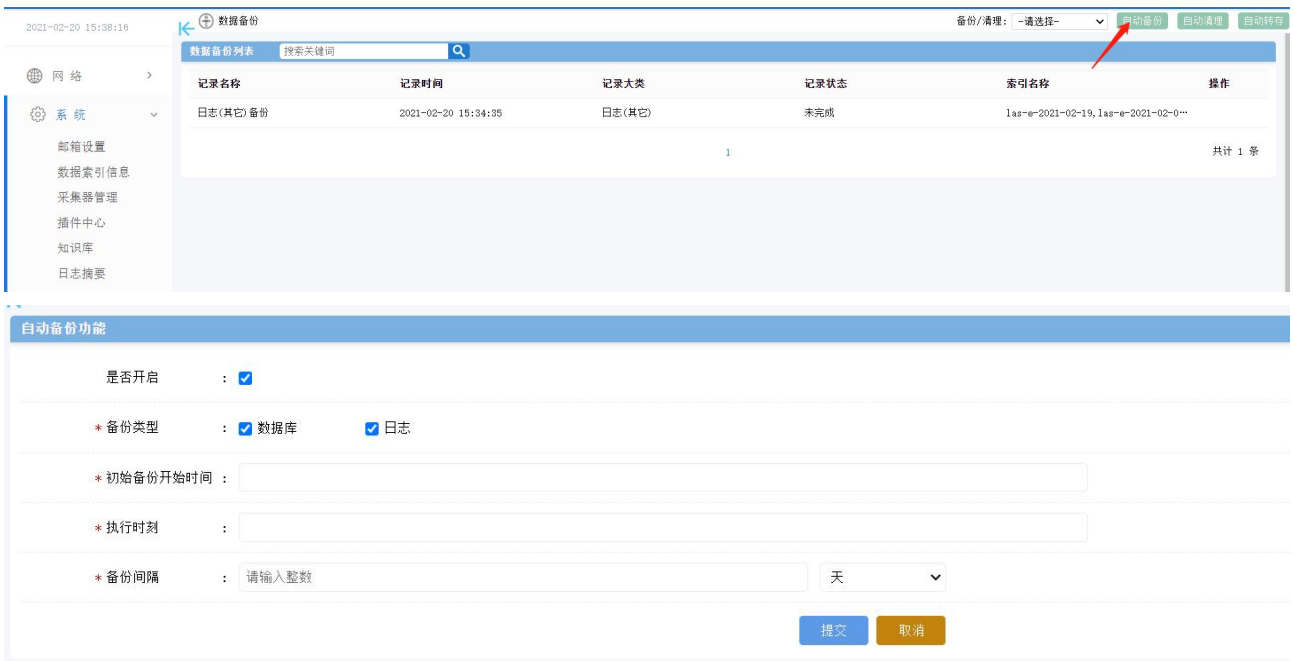


12.9.1 手动备份

按需选择页面右上角‘备份/清理’项，系统提示：确定备份此项吗？点击‘确定’完成手动备份操作。

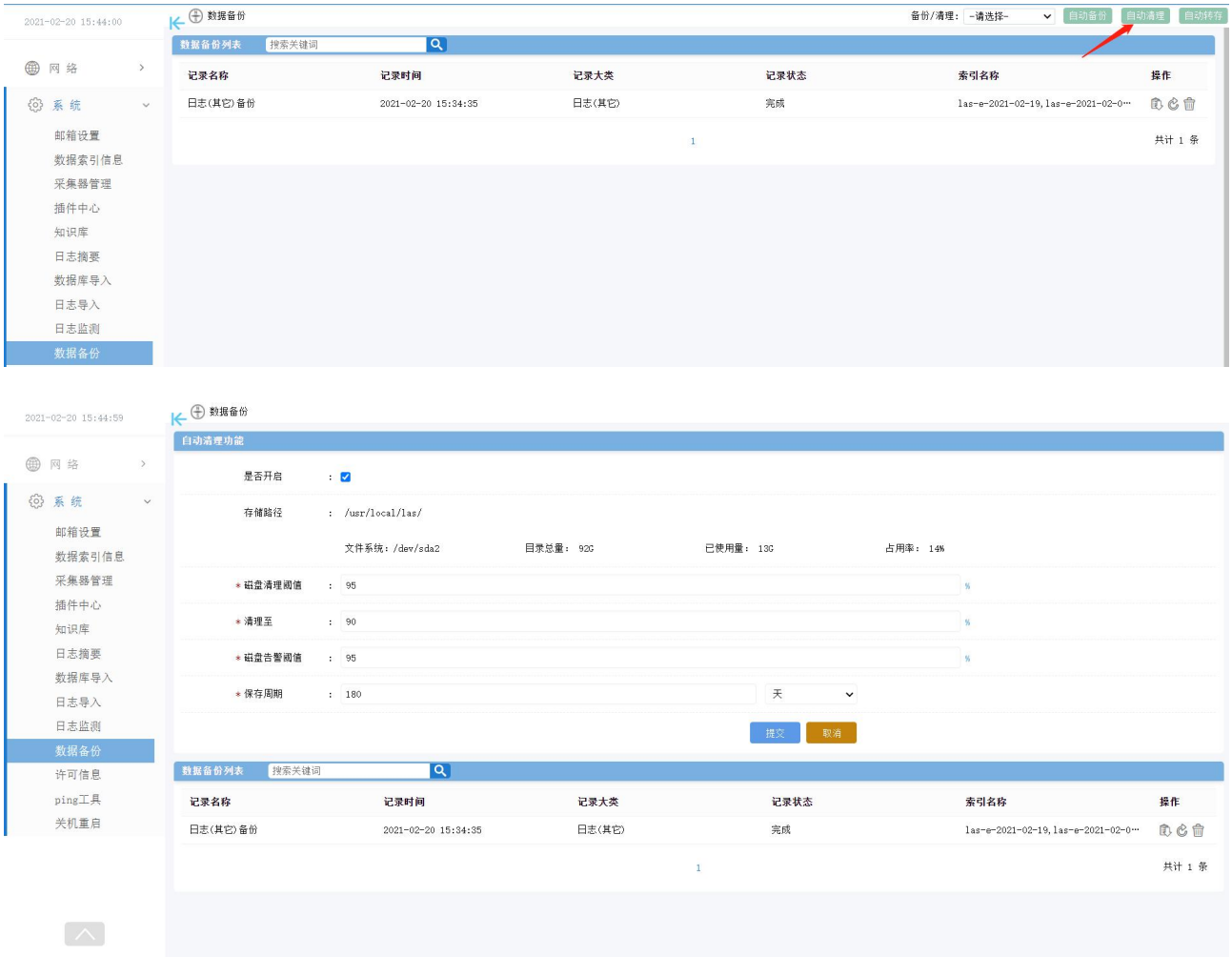
12.9.2 自动备份

点击右上角‘自动备份’按钮，显示自动备份模块，按照需要勾选或填写提交项信息，点击‘提交’按钮完成自动备份操作。



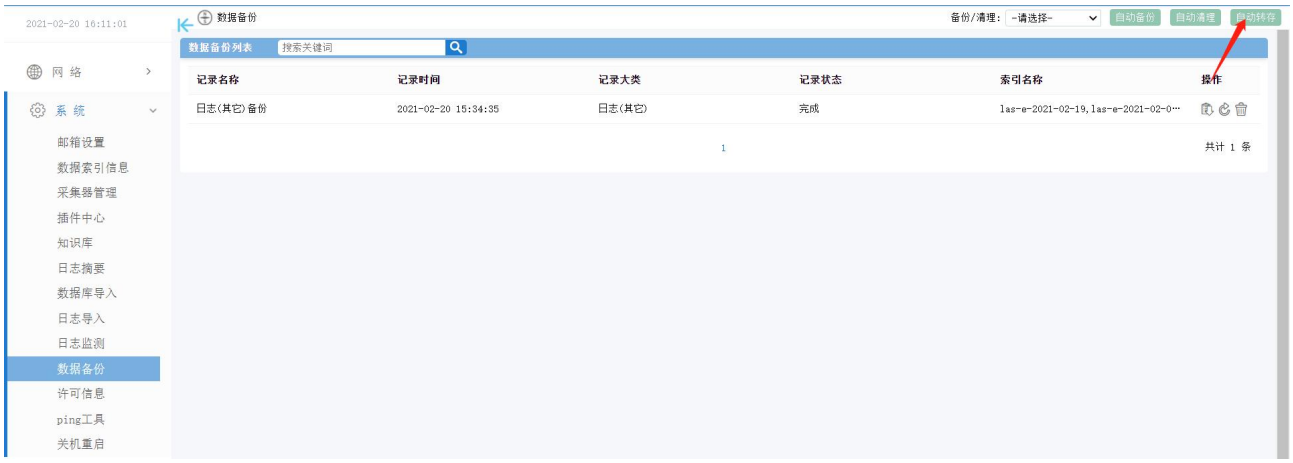
12.9.3 自动清理

点击右上角‘自动清理’按钮，显示自动清理模块，按照需要勾选或填写提交项信息，点击‘提交’按钮完成自动清理操作。



12.9.4 自动转存

点击右上角“自动转存”按钮，显示自动转存功能，按照需要勾选或填写提交项信息，点击‘提交’按钮完成自动转存操作。



12.10 许可信息

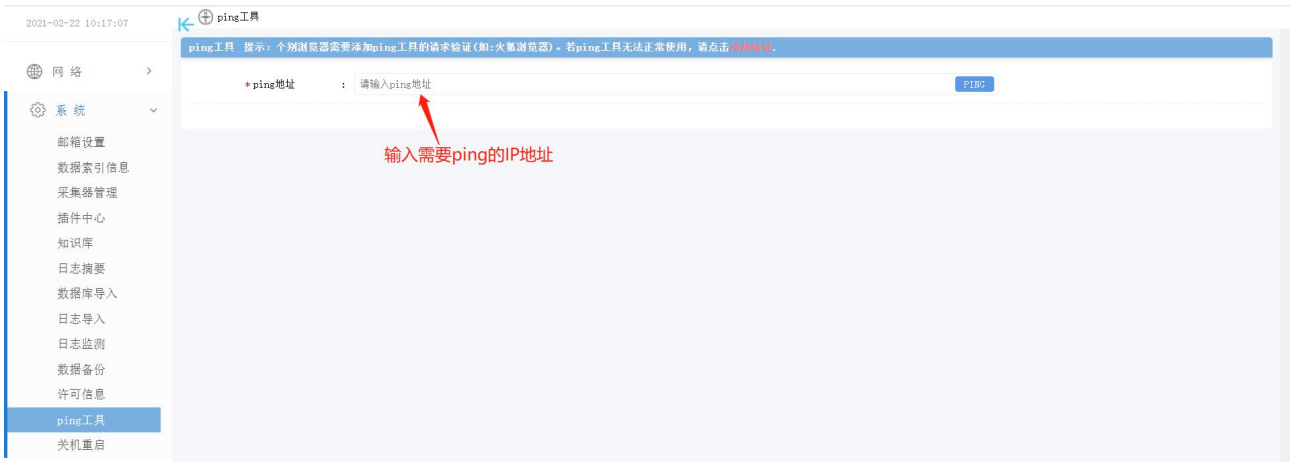
菜单项‘系统’→‘许可信息’子项。进入系统许可信息模块，可查看系统版本和授权信息，也可在‘注册码’信息表中上传注册文件，点击‘授权’完成系统的授权操作。

12.10.1 系统升级

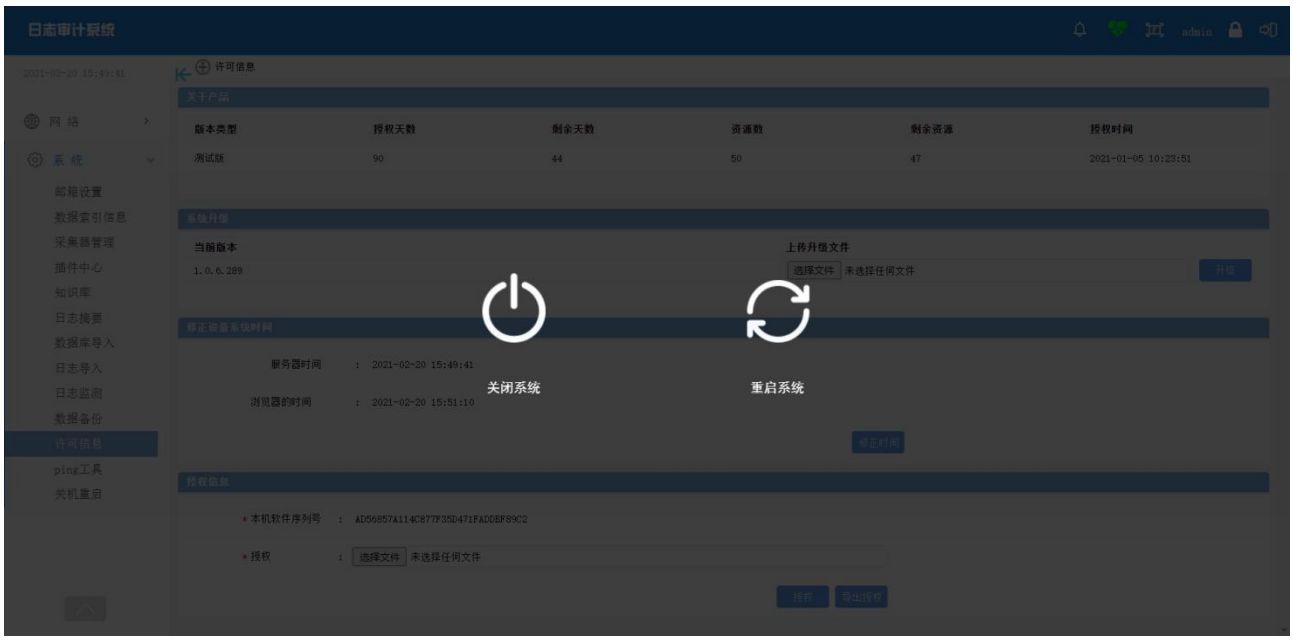
菜单项‘系统’→‘许可信息’子项。进入系统升级模块，可查看系统版本和升级信息，也可‘系统升级’表中上传升级文件，点击‘升级’完成系统的升级操作。

12.11Ping 工具

菜单项‘系统’→‘ping 工具’子项。进入系统 ping 工具模块，可查看设备网络之间连通性。



12.12 关机重启


日志审计系统
admin
许可信息
关于产品
版本类型
授权天数
剩余天数
资源数
剩余资源
授权时间
测试版
90
44
50
47
2021-01-05 10:23:51
网 络
系 统
邮箱设置
数据索引信息
采集器管理
插件中心
知识库
日志摘要
数据库导入
日志导入
日志监测
数据备份
许可信息
ping工具
关机重启
系统升级
当前版本
1.0.6.289
上传升级文件
选择文件
未选择任何文件
升级
修正设备系统时间
服务器时间 : 2021-02-20 15:49:41
浏览器的时间 : 2021-02-20 15:51:10
关闭系统
重启系统
修正时间
授权信息
本机软件序列号 : AD56B57A114C877F35D471FADDBF89C2
授权 : 选择文件 未选择任何文件
授权
导出授权